Statement for the Record

Dr. Charles E. McQueary
Under Secretary for Science and Technology
Department of Homeland Security

Before the U.S. House of Representatives
Committee on Science

February 16, 2005

Table of Contents

Introduction

Good morning. Chairman Boehlert, Congressman Gordon, and distinguished Members of the committee. It is a pleasure to be with you today to discuss the research and development activities of the Department of Homeland Security's (DHS's) Science and Technology (S&T) Directorate.

The Nation's advantage in science and technology is key to securing the homeland. The most important mission for the Science and Technology Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently – these men and women are my customers.

When I last reported to you about our activities, we were just over one year old as a Department. Since my last report, the Science and Technology Directorate has:

1) Developed and documented a robust Research, Development, Testing and Evaluation (RDT&E) process that includes risk-based planning for the S&T Directorate's programs and initiatives.
2) Continued daily operation, maintenance and deployment of BioWatch, a biological agent detection system, to protect the nation's major population centers from the threat and ramifications of a bioterrorist attack. BioWatch also provided support during the G8, Democratic National Convention and Republican National Convention.
3) Selected four cities for the deployment of a new pilot program entitled the Regional Technology Integration (RTI) initiative (formerly "Safe Cities"). The selected cities include: Memphis, TN; Anaheim, CA; Cincinnati, OH; and Seattle, WA. RTI provides an integrated urban all-hazards detection and emergency response system.
4) Established a dedicated National Bioforensics Center to support ongoing Federal Bureau of Investigation (FBI) and other law enforcement investigations.
5) Established the National Visualization and Analytics Center and the Biological Knowledge Center to improve the analysis of information and close knowledge gaps.
6) Established a test and evaluation capability for Radiological/Nuclear Countermeasures at the Nevada Test Site.
7) Selected over 100 undergraduate and graduate students, in the fall of 2004, for grants to assist in the study of science and technology issues that support the homeland security mission.
8) Launched three Homeland Security Centers of Excellence to date with negotiations taking place for a fourth and the solicitation released for the fifth.
9) Issued ten major R&D solicitations to industry and academia through the first 20 months and issued more than 200 contracts for research work to date.
10) Collaborated with and assisted other components of the Department to enhance their abilities to meet their missions and become active contributors in interagency working groups — all while staffing this Directorate with some of this country's brightest and most dedicated people.
11) Awarded four SAFETY Act designations and certifications, received and responded to 72 full applications and 166 pre-applications, and worked to streamline the process.

12) Stood up the Department's Office of Interoperability and Compatibility to address the wide range of public safety interoperability programs and efforts currently spread across Homeland Security.
13) RapidCom improved incident-level, interoperable emergency communications in ten high-threat urban areas by helping to establish command-level interoperability within an hour or less.
14) Completed Phase I of the Counter-MANPADS Program and initiated Phase II which will advance the studies initiated in phase I, build system prototypes and conduct effectiveness testing.

I continue to be energized by and proud of the scientists, engineers, managers, and support staff in the Science and Technology Directorate. We have accomplished a great deal in a short amount of time and are positioning the Directorate to make continuing contributions to the homeland security mission of the Department.

However, the threats to our homeland remain diverse and daunting. We must constantly monitor current and emerging threats and assess our vulnerabilities to them, develop new and improved capabilities to counter them, and mitigate the effects of terrorist attacks should they occur. The Science and Technology Directorate must also enhance the conventional missions of the Department to protect and provide assistance to civilians in response to natural disasters, law enforcement needs, and other activities such as maritime search and rescue. Basically we assist in making DHS operations science based, intelligence informed and technology enabled.

The Science and Technology Directorate's Research, Development, Testing, and Evaluation Process

As I just mentioned, one of the Directorate's accomplishments over the last year was the development and documentation of a robust Research, Development, Testing, and Evaluation (RDT&E) process. The goal of the RDT&E process is to provide a clearly defined, repeatable method for assessing needs and risk, planning, allocating resources and executing programs to produce high-impact, cost-effective and critically needed homeland security technology solutions.

The S&T Directorate's RDT&E process uses a risked-based approach to planning and is oriented toward identifying critical capability gaps before attempting to identify or develop technology solutions. In developing solutions, the process engages the end-user throughout requirements definition, development, testing and transition. The process considers the product life cycle from the outset, including planning and budgeting for production, deployment, operations and support. It is this process which allows us to prioritize both within and across fields.

RDT&E consists of four main sub-processes: 1) needs and risk assessment, 2) strategic planning, 3) program definition, and 4) program execution. The first two sub-processes ensure that the Science and Technology Directorate considers user needs, available intelligence, big-picture risks, national goals and inputs from other external agencies and advisory bodies to establish its annual RDT&E program. The second two sub-processes provide a framework for

program execution using the best available systems engineering and program management techniques.

Science and Technology Directorate Organization

We have four key offices in the Science & Technology Directorate, each of which has an important role in implementing the Directorate's research, development, testing and evaluation (RDT&E) activities. These offices are: Plans, Programs, and Budget (PPB); Office of Research and Development (ORD); Homeland Security Advanced Research Projects Agency (HSARPA); and Systems Engineering and Development (SED). In addition, the S&T Directorate houses the Office of Weapons of Mass Destruction Operations and Incident Management to offer scientific advice and support to meet operational needs.

Crosscutting the four key offices, the Science and Technology Directorate implements its activities through focused portfolios that address biological, chemical, explosives, radiological and nuclear, and cyber threats; support the research and development needs of the operational units of the Department; support the development of standards and interoperability; develop an enduring R&D capability for homeland security; and receive valuable input from private industry and academia as well as national and Federal laboratories. I will talk about the offices first and then about the portfolios.

Office of Plans, Programs, and Budget

PPB is organized into the portfolios I just mentioned, each of which is focused on a particular discipline or activity; taken together, these portfolios span the Directorate's mission space. As I will cover the portfolios in detail later in this testimony, I will limit myself here to a summary explanation. The staff of each portfolio is charged with being expert in their particular area; with understanding the activities and capabilities extant in Federal agencies and across the broad research and development community; and with developing a strategic plan for their particular portfolio, to include near-, mid-, and long-range research and development activities. In addition, we have staff that is charged with understanding the threat from a technical perspective, with integrating the various portfolios into a coherent overall plan, and with developing the corresponding budget and monitoring its financial execution.

Finally, PPB is responsible for executing the Directorate's implementation responsibilities for the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act.

Office of Research and Development

ORD provides the nation with an enduring capability in research, development, demonstration, testing and evaluation of technologies to protect the homeland. ORD builds enduring RDT&E capability through stewardship of the homeland security complex- people, places, and programs – to anticipate, prevent, respond to and recover from terrorist attacks.

Activities within ORD address the resources that can be brought to bear to better secure the homeland through the participation of universities, national laboratories, Federal laboratories and research centers.

Homeland Security Advanced Research Projects Agency

HSARPA is an external research-funding arm of the Science and Technology Directorate. It has at its disposal a full range of contracting vehicles and the authority under the Homeland Security Act of 2002 to engage businesses, federally funded research and development centers, universities, and other government partners in performing its mission to gather, generate and develop ideas, concepts and advanced technologies to protect the homeland.

HSARPA's mission is to support basic, applied, and advanced homeland security research to promote revolutionary changes in technologies that would promote homeland security; advance the development, testing and evaluation, and deployment of homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities. Its customers are state and local first responders and Federal agencies that are allied with homeland security such as the U.S. Coast Guard, U.S. Secret Service, U.S. Citizenship and Immigration Services, Federal Emergency Management Agency, and others.

About 60 percent of the Science and Technology Directorate's appropriation in FY 2005 will be executed directly through the private sector, with HSARPA managing about 40% of that.

Office of Systems Engineering and Development

SED is tasked with leading the implementation and transition of large-scale or pilot systems to the field through a rapid, efficient and disciplined approach to project management.

One of the Science and Technology Directorate's challenges is to evaluate a wide spectrum of military and commercial technologies so rapid, effective and affordable solutions can be transitioned to the Department's customers that include first responders and Federal agencies. In some cases, military technologies could be candidates for commercialization, but rigorous systems engineering processes need to be applied to ensure a successful transition. SED's role is to identify and then, in a disciplined manner, reduce risks associated with such technologies to ready them for deployment to the field. In doing so, the office must view each technology through the prism of affordability, performance and supportability — all critical to end-users.

SED must weigh considerations such as the urgency for a solution, consequences of the threat, safety of the product, and lifecycle support as new products are introduced. Products must be user friendly, have a minimum of false alarms, require little or no training and consistently provide accurate results. SED will demonstrate and test solutions before they are released to the field, and will validate that those solutions meet user expectations. SED also operates our Countermeasures Test Bed capability, which provides end-user "in the loop" operational testing and evaluations to the Directorate's portfolios.

Office of Weapons of Mass Destruction Operations and Incident Management

We created the Office of Weapons of Mass Destruction Operations and Incident Management as the Science and Technology Directorate's operational arm for DHS support to incident management. Through this Office, the Science and Technology Directorate exercises its scientific and technical leadership role under the National Response Plan. This Office provides rapid scientific and technical expertise and executive decision support to the Secretary, DHS response units, interagency partners, and the state and local jurisdictions that form the front line response to chemical, biological, radiological, nuclear and high-explosives threats and incidents.

Results from Current Research and Development (R&D) Spending and FY 2006 Plans: Portfolio Details

The Science and Technology Directorate has organized its efforts into research and development portfolios that span the set of product lines of the Directorate. Four portfolios address the development of countermeasures for specific terrorist threats: Biological Countermeasures, Chemical Countermeasures, Explosives Countermeasures, and Radiological and Nuclear Countermeasures.

In addition to the countermeasures portfolios, four portfolios support the operational units of the Department: Border and Transportation Security (BTS), Emergency Preparedness and Response (EPR), United States Coast Guard (USCG) and United States Secret Service (USSS) portfolios.

The Standards, Emerging Threats, and Rapid Prototyping portfolios crosscut all terrorist threats and enhance the research and development conducted in the countermeasures portfolio.

The Directorate has three portfolios that focus on the protection of the nation's vital infrastructure: Threat and Vulnerability, Testing and Assessment, Critical Infrastructure Protection and Cyber Security.

The S&T Directorate addresses other areas as well:

- Our University and Fellowship Programs portfolio addresses the need to build an enduring science and technology capability and support United States leadership in science and technology.

- Our Counter-MANPADS program is seeking to improve technologies to protect commercial aircraft from the threat of MAN-Portable Air Defense Systems (MANPADS).

- The Office of Interoperability and Compatibility (OIC), managed by the Science and Technology Directorate, oversees the wide range of public safety interoperability programs and efforts currently spread across Homeland Security, including critical interoperability issues relating to public safety and emergency response, including communications, equipment, training, and other areas as needs are identified.

- The Domestic Nuclear Detection Office (DNDO) is being established to be the single entity responsible for coordinating and extending efforts in nuclear/radiological detection. This office will consolidate functions within the Department of Homeland Security and establish strong linkages across the interagency for the deployment of a national domestic nuclear detection architecture, the conduct of transformational research and development, and the establishment of protocols and training for the end users of equipment developed and deployed through the new office.

At this time I would like to briefly describe some of our accomplishments to date and our FY 2006 plans. As can be seen in the following chart, we have an overall FY 2006 budget request of $1.368 billion, which is an increase of $253.0 million (22.7 percent) over the FY 2005 levels. The request includes the construction of the National Bio and Agrodefense Facility, the development of a Low-Volatility Agent Warning System, a Radiological/Nuclear Countermeasures Testing and Evaluation Complex, additional development of Counter-Man-Portable-Air-Defense Systems (C-MANPADS), and the consolidation of the Department's RDT&E activities.

	FY 2004	FY 2005	Proposed	Increase/Decrease	
	Actual	Enacted	FY 2006	From FY 2005 to 2006	
BUDGET ACTIVITY	Amounts (millions)	Amounts (millions)	Amounts (millions)	Amounts (millions)	Percent Increase
Management and Administration	43.9	68.6	81.4	12.8	18.7%
Bio Countermeasures	162.6	362.6	362.3	(0.3)	-0.1%
NBACC*	4.3	35.0	-	(35.0)	-100.0%
Chemical Countermeasures	22.9	53.0	102.0	49.0	92.5%
Explosives Countermeasures	7.0	19.7	14.7	(5.0)	-25.4%
Radiological and Nuclear Countermeasures	105.7	122.6	19.0	(103.6)	-84.5%
Domestic Nuclear Detection Office			227.3	227.3	
Threat and Vulnerability, Testing and Assessments	58.7	65.8	47.0	(18.8)	-28.6%
Standards	32.2	39.7	35.5	(4.2)	-10.6%
Support of Department of Homeland Security Components	20.8	54.7	93.7	39.0	71.3%
University and Fellowship Programs	22.0	70.0	63.6	(6.4)	-9.1%
Emerging Threats	11.2	10.7	10.5	(0.2)	-1.9%
Rapid Prototyping	68.4	76.0	20.9	(55.1)	-72.5%
Counter MANPADS	16.7	61.0	110.0	49.0	80.3%
SAFETY Act	-	10.0	5.6	(4.4)	-44.0%
Office of Interoperability and Compatibility	-	21.0	20.5	(0.5)	-2.4%
Critical Infrastructure Protection	12.1	27.0	20.8	(6.2)	-23.0%
Cyber Security	10.3	18.0	16.7	(1.3)	-7.2%
Research and Development Consolidation	-	-	116.9	116.9	
Total enacted appropriations and budget estimates	598.8	1,115.4	1,368.4	253.0	22.7%

*Includes construction costs

Biological Countermeasures

Biological threats can take many forms and be distributed in many ways. Aerosolized anthrax, smallpox, foot and mouth disease, and bulk food contamination are among the threats that can have high consequences for humans and agriculture. Our Biological Countermeasures portfolio uses the nation's science base to prevent, protect, respond to, and recover from bioterrorism events. This portfolio provides the science and technology needed to reduce the probability and potential consequences of a biological attack on this nation's civilian population, its infrastructure, and its agricultural system. Portfolio managers and scientists are developing and implementing an integrated systems approach with a wide range of activities, including vulnerability and risk analyses to identify the need for vaccines, therapeutics, and diagnostics; development and implementation of early detection and warning systems to characterize an attack and permit early prophylaxis and decontamination activities; and development of a national bioforensics analysis capability to support attribution of biological agent use.

In FY 2004 and FY 2005, the Biological Countermeasures portfolio:

- Deployed the BioWatch environmental sensor system to protect our nation's cities from the threat and ramifications of a bioterrorist attack. BioWatch activities were significantly increased during the National Code Orange Alert (December 2003-January 2004), with twice daily samplings in the high threat cities, additional collectors for special New Year's events and Bowl Games, and deployment of temporary BioWatch systems to non-BioWatch cities of special concern. BioWatch also provided field and laboratory support to the G8, the Democratic National Convention and the Republican National Convention in Boston and New York.
- Engaged in creating more near real-time monitoring of critical infrastructure facilities such as major transportation hubs. New infrastructure protection efforts include shorter response time biological agent detection capabilities for BioWatch. This pilot is in the process of being deployed in New York City and will join a three-to-five expansion of the number of collectors in that city.
- Initiated the design of the National Biosurveillance Integration System (NBIS) as part of an interagency process. Recently completed in the first quarter of FY 2005, we will work with the Information Analysis and Infrastructure Protection (IAIP) Directorate to implement this system.
- Conducted preliminary analyses, using the reference scenario approach recommended by Homeland Security Presidential Directive (HSPD)-10 for understanding the requirements of an integrated national biodefense architecture, of four baseline reference cases: a large outdoor release of a non-contagious agent (anthrax); a large indoor release of a contagious agent (smallpox); contamination of a bulk food supply; and two highly virulent agricultural attacks, one on livestock (Foot and Mouth Disease) and the other on plants (soy bean rust).
- Established the Biodefense Knowledge Center, an operational hub for enabling collaboration and communication within the homeland security complex. The Biodefense Knowledge Center will meet the operational and planning requirements of government decision-makers and program planners, the intelligence community, law enforcement officers, public health practitioners, and scientists. Specific capabilities offered to these

end-users include knowledge services, modeling and simulation, situational awareness and a pathway to accelerate research and development.

In FY 2006, the Biological Countermeasure portfolio plans to:

- Complete the three high level architectures initiated in FY 2005 (multiple small attacks, an engineered organism, and an intentional spread of a zoonotic disease), identifying key requirements for each major element, a "report card" on the current and projected status in that area and performing detailed design tradeoffs for those areas in which DHS has execution responsibility.
- Complete the first formal risk assessment required under HSPD-10 and close many of the key remaining experimental gaps in our knowledge of the classical biological threat agents. Near-, mid-, and long-term plans for dealing with engineered agents will be developed, and R&D on addressing the gaps in responding to modified organisms (e.g., antibiotic resistant) initiated.
- Complete the deployment of Generation 2 BioWatch systems to the top threat cities while continuing to operate and optimize already extant BioWatch systems. Complete test and evaluation of laboratory prototypes of the Generation 3 BioWatch detection systems which will be ready for down-selection those which will go on to develop fieldable prototypes in FY 2007.
- Continue operation of the interim National Bioforensic Analysis Center. International Organization for Standardization (ISO) certification is expected to have been achieved, giving the analyses conducted additional credibility and authenticity in both the national and international community and courts of law. R&D will continue on the physical and chemical signatures of the "matrix" materials associated with biological agents so as to develop methods for understanding tell-tale remnants of enrichment media, culture conditions, metabolites, and dispersion technology.
- Continue operation of the Plum Island Animal Disease Center (PIADC) and essential upgrades to the facility and initiate design of the National Bio and Agrodefense Facility (NBAF). R&D will continue on next generation vaccines and antiviral therapeutics for foot and mouth disease (FMD) and other high priority foreign animal diseases.
- Continue to develop bioassays for FMD and look-alike animal diseases. The initial agricultural forensic capability established in FY 2004 at PIADC will be enhanced and epidemiologic capability added. A High Throughput Diagnostics Demonstration will be initiated to work with regional and state laboratories to demonstrate a capability of analyzing thousands of samples per day in support of response to a suspected case or an outbreak. A FMD table top exercise of DHS Directorates will be initiated, and development of a coupled epidemiological and economic model for FMD will begin. The end-to-end systems study initiated in FY 2004 for Soybean Rust and FMD will be completed, and system studies initiated for highly pathogenic avian influenza.

National Bio-Defense Analysis and Countermeasures Center (NBACC)

The NBACC, a key component of the *National Strategy for Homeland Security,* addresses the need for scientific research to better anticipate, prevent, and mitigate the consequences of biological attacks. The need for the NBACC facility is further defined in the Presidential

Directive *Biodefense for the 21st Century*, the Nation's blueprint for future biodefense programs. The NBACC's mission will support two pillars of this blueprint – threat awareness and surveillance and detection. The NBACC is made up of two centers, the Biological Threat Characterization Center and the National Bioforensic Analysis Center to carry out these missions. Specifically, NBACC's mission is to:

- Understand current and future biological threats, assess vulnerabilities, and determine potential impacts to guide the research, development, and acquisition of biodefense countermeasures such as detectors, drugs, vaccines and decontamination technologies; and
- Provide a national capability for conducting forensic analysis of evidence from bio-crimes and terrorism to attain a "biological fingerprint" to identify perpetrators and determine the origin and method of attack.

In FY 2004, the Department completed the planning and conceptual design of the NBACC facility. Additionally, the Department has been working through the National Environmental Policy Act (NEPA) process during the year, which culminated in the signing of the Record of Decision in January 2005 of the Final Environmental Impact Statement (EIS) for the construction project and subsequent operations. It was decided to delay the award of any contracts for design and construction until further in the EIS process. As the public concerns are analyzed and considered it is anticipated that contracts will be awarded in FY 2005 to initiate design and construction of the NBACC facility

In FY 2005, the solicitations of contracts for the design and construction of the NBACC facility are expected to be awarded. The design of the NBACC facility will commence in March 2005. $35M was appropriated to obligate funds for award of the construction contract in the fourth quarter of FY 2005. Construction of the facility is planned for completion by the fourth quarter of FY 2008.

In FY 2006, funding was not requested for the construction of the NBACC facility.

Chemical Countermeasures

The National Research Council Report *Making the Nation Safer* points out that "chemicals continue to be the weapon of choice for terrorist attacks." Until recently, the chemical threat spectrum was limited to the threats posed by chemical warfare agents (CWAs) in a military context and the threats posed by the accidental or inadvertent release of toxic materials in the homeland domain. Now, the chemical threat spectrum has expanded to include chemical warfare agents (CWAs), toxic industrial chemicals (TICs), non-traditional agents (NTAs) and toxins. As with the threat materials themselves, the range of potentially attractive targets is large. The potential for chemical warfare agents and emerging threat agents constitute a broad range of threats that may be applied to virtually any civilian target.

The Chemical Countermeasures portfolio works to enhance the nation's capability to anticipate, prevent, protect, respond to and recover from chemical threat attacks through interagency leadership and conduct of innovative research, development, and technology transition. The

portfolio works through the interagency environment to shape a comprehensive strategy for enhancing the Nation's defensive posture and to develop bases for enhanced R&D program integration and leverage. The R&D activities include prioritization of efforts among the many possible chemical threats and targets, and development of new detection and forensic technologies and integrated protective systems for high-value facilities such as airports and subways. These activities are informed by end-user input and simulated exercises.

In FY 2004 and FY 2005, the Chemical Countermeasures portfolio:

- Conducted preliminary activities toward the development of a Chemical Security Analysis Center (CSAC) that will provide threat awareness and assessment. An overall structure, similar to that characterizing the NBACC and its supporting threat characterization, forensics, knowledge management and reachback, is envisioned.
- Initiated system studies around three defining scenarios: indoor chemical agent release, outdoor toxic industrial chemical release, and release of toxin in the water system.
- Initiated three demonstration projects: the Facility Restoration Demonstration Project to develop and demonstrate a capability to rapidly restore a facility that has been contaminated with a classical chemical agent or persistent toxic industrial chemical (TIC); a Water Security Demonstration to identify and characterize technologies with the potential to provide warning of chemical contamination of the water system; and a National Security Special Event (NSSE) Deployable Detection System Demonstration to develop a flexible architecture chemical detection system that can be utilized for the warning and situational awareness of chemical threats in temporary deployments.
- Initiated key development programs targeting leap-ahead advancements in detection capabilities. These programs will develop two principal capabilities: a facility monitoring detector and a responder detection tool. In both cases, the detectors will provide detection and discrimination of up to 20 different chemical threats, including classical chemical warfare agents (CWAs) and toxic industrial chemicals (TICs) in a single unit across a wide range of concentrations.

In FY 2006, the Chemical Countermeasure portfolio plans to:

- Reach full operational status at the CSAC where chemical threat databases will be centrally located and accessible.
- Complete technology down-select and draft candidate decontamination protocols in concert with the Environmental Protection Agency (EPA) through the Facility Restoration Technology Demonstration. Transition the Water Security Demonstration to EPA for continuation and conduct technology down-select for the next-generation deployable capability through the NSSE Technology Demonstration.
- Complete the critical design review of technologies for the rapid facility monitor and the first responder tool and conduct a technology down-select supporting prototype selection and build.
- Initiate and demonstrate operational solutions to the challenge of decontaminating non-traditional agents and initiate next-generation decontamination research.

Explosives Countermeasures

The Explosives Countermeasures portfolio addresses the threat that terrorists will use explosives in attacks on buildings, critical infrastructure, and the civilian population of the United States. The Science and Technology Directorate's Explosives portfolio has been closely coordinated with the activities ongoing in the Transportation Security Administration to ensure that research and development (R&D) activities are complementary, not duplicative; in FY 2006, these activities will be consolidated within the S&T Directorate. R&D priorities in the Explosives Countermeasures portfolio focus on the detection of vehicle bombs and suicide bombers and on providing the science and technology needed to significantly increase our ability to prevent an explosives attack on buildings, infrastructure or people.

In FY 2004 and FY 2005, the Explosives Countermeasures portfolio:

- Addressed terrorist attacks against buildings and the general population. The portfolio initiated the development of a prototype explosive detector for vehicle bombs, and accelerated the development of hardened overhead storage bins for passenger aircraft. Additionally, it initiated a survey and evaluation of commercial-off-the-shelf equipment to detect, interdict and mitigate the consequences of suicide bombers and vehicle bombs, and conducted a cost-benefit analysis of approaches to aircraft hardening.
- Funded the demonstration in FY 2005 of the capabilities identified in FY 2004, used to provide the ability to detect, interdict, and mitigate the consequences from suicide bombers, truck, and car bombs approaching high profile targets and densely populated areas.

In FY 2006, the Explosives Countermeasure portfolio plans to:

- Continue to consolidate explosives management functions as outlined above. Efforts will focus on developing the ability to detect, interdict and mitigate the consequences from suicide bombers, truck and car bombs approaching high profile targets and densely populated areas. Additonally, the portfolio will provide the ability to detect, interdict and mitigate the consequences of explosives and weapons on aircraft transporting (domestic and foreign inbound) passengers and their baggage as well as cargo containers/bays. Specific areas to be pursued are infrastructure protection, suicide bombers/leave behind improvised explosive devices, and vehicle bombs.

Radiological and Nuclear Countermeasures

Potential radiological and nuclear threats range from the deliberate dispersal of small amounts of radioactive material to the detonation of an improvised or stolen nuclear weapon to an attack on our nuclear power industry. Our Radiological and Nuclear Countermeasures portfolio provides the science and technology needed to reduce both the probability and the potential consequences of a radiological or nuclear attack on this nation's civilian population or our nuclear power facilities. Many of the on-going activities conducted in the Radiological/Nuclear

Countermeasures Portfolio are being transferred in FY 2006 to the Domestic Nuclear Detection Office (DNDO). Those activities are indicated in the next section.

In FY 2004 and FY 2005, the Radiological/Nuclear Countermeasures portfolio:

- Formally assumed management of the Port Authority of New York and New Jersey radiation detection test bed from the Department of Energy in August, 2003. Following the transfer, the portfolio broadened the project scope beyond testing and evaluating individual pieces of technology to a systems approach, including response protocols and operational concepts. This program has been renamed the Countermeasures Test Bed to more accurately reflect that this program supports DHS's enduring operational testing and evaluation needs for all threat countermeasures technology, not just Radiological/Nuclear threats.
- Focused detection technology efforts on the detection of shielded special nuclear material (SNM) in cargo containers, based on the detection of both neutrons and delayed high-energy fission product gamma rays, and a portable neutron source, based on a mixed alpha-Be source in a switchable configuration for use in active interrogation; both currently are still in conceptual design and experiment phases.
- Preplanned product improvement efforts in this area were directed towards improvements in two current Customs and Border Protection-deployed radiographic imaging systems. This included software improvements and systems upgrades for local data integration, threat image projection (TIP), and assisted imaging processing (AIP).
- Incident management/recovery efforts include a joint DHS/HSARPA and DoD/DARPA (Department of Defense/Defense Advanced Research Projects Agency) project focusing on radiological and nuclear decontamination, consisting of four main tasks: (1) Radionuclide capture decontamination; (2) Wide area radionuclide decontamination; (3) Verification; and (4) Modeling.
- A major goal of FY 2005 is to establish a test and evaluation capability at the Nevada Test Site (NTS) for testing against SNM, and, as appropriate, to test and evaluate relevant FY 2005 prototype technologies developed in the portfolio's programs.

In FY 2006, the Radiological/Nuclear Countermeasure portfolio plans to:

- Redirect all detection related missions and corresponding funding to the establishment of the Domestic Nuclear Detection Office. The remaining, non-detection research and development will continue to be funded through the Radiological/Nuclear Countermeasures portfolio. The two programmatic thrust areas remaining are Incident Management and Recovery, and Attribution and Forensics on Contaminated Evidence (formerly part of the Systems Analysis and Pilot Deployments programmatic area).
- Complete the laboratory improvements that are necessary to carry out the attribution mission.
- Complete all field studies for the New York City Urban Dispersion Program with a technology transfer following to NYC Office of Emergency Management in late 2006.

Domestic Nuclear Detection Office

The risk that terrorists will acquire and use a Nuclear/Radiological device is one of the gravest threats that confronts the Nation. Acquiring nuclear weapons and materials is the hardest step for terrorists to take, and the easiest for us to stop. By contrast, every subsequent step in the process becomes easier for the terrorists, and harder for us to stop. Our defensive posture must begin with eliminating excess stocks of nuclear material and weapons throughout the world, protecting existing stocks from theft or diversion, and detecting illicit movement of nuclear/radiological material overseas before it reaches our borders. However, recognizing that even the best efforts to secure weapons and fissile material may not achieve 100 percent success, we must supplement these efforts abroad with a stronger layer of protection at home.

We must move swiftly to deploy a well-integrated system of detectors for nuclear/radiological materials and improve this system over time. While such a system will never be foolproof, it can dramatically improve the probability that we could detect illicit nuclear or radiological materials being brought covertly into position for use by an adversary. The gravity of the risk demands the focused, aggressive program envisioned here, with its mutually supportive elements of deploying and knitting together current technology so as to exact the greatest possible protection for our population while working continuously to improve that technology over time.

Since 9/11, many agencies have expanded their activities and operations to help build the domestic layers of the Nation's defense against nuclear terrorism. To optimize and advance these efforts, a new national-level, jointly staffed Domestic Nuclear Detection Office (DNDO) is being created to coordinate and extend the efforts in nuclear/radiological detection. This office will consolidate functions within DHS and establish strong linkages across the interagency for the deployment of a national domestic nuclear detection architecture, the conduct of transformational research and development (R&D), and the establishment of protocols and training for the end users of equipment developed and deployed through the new office. The office will further serve as the primary entity to

- Further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on any attempt to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States.

- Enhance and coordinate the nuclear detection efforts of Federal, State, and local governments and the private sector to ensure a managed, coordinated response;

- Jointly establish and coordinate additional protocols and procedures for domestic use to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Director of the Federal Bureau of Investigation (FBI), the Secretary of Defense, the Secretary of Homeland Security, the Secretary of Energy, and other appropriate officials or their designees for appropriate action by law enforcement, military, emergency response, or other authorities;

- Jointly develop and coordinate an enhanced global nuclear detection architecture with the following implementation: (i) the DNDO will be responsible for the implementation of the domestic portion of the global architecture, (ii) the Secretary of Defense will retain responsibility for implementation of DOD requirements, and (iii) the Secretaries of Defense, Energy, and State will maintain their respective responsibilities for policy guidance and implementation of the overseas portion of the global architecture, which will be implemented consistent with applicable law and relevant international conditions.

- Conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development efforts to support the policy;

- Support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments as well as provide information to these entities; and

- Further enhance and maintain continuous awareness by analyzing information from all DNDO mission-related detection systems.

Building upon the redirected base funding of $113 million for detection related RDT&E in the Radiological/Nuclear Countermeasures Portfolio, the FY 2006 request includes an additional $105.0 million to support the DNDO's mission and objectives (plus the $9 million requested increase for the Radiological/Nuclear Countermeasures Test and Evaluation Complex (Rad/NUc CTEC) discussed later in the FY 2006 Science and Technology Directorate Initiatives section.

Although the DNDO is principally focused on domestic detection, its coordinating work will enhance U.S. efforts overseas through the design of a global architecture implemented under current agency responsibilities. The new investments will speed the development and improvement of equipment and protocols, much of which will be applicable overseas.

Because multiple agencies share the resources or expertise necessary for the success of the office, the DNDO will be located within the Department of Homeland Security (DHS), but will be jointly staffed with representatives from DHS, the Department of Energy (DOE), the Department of Defense (DoD), and the Federal Bureau of Investigation (FBI), with coordination between the Department of Justice (DOJ), the Department of State (DOS), the Intelligence Community (IC), and other departments as needed.

The DNDO mission will be carried out through an organization that includes a Director supported by five major offices: Systems Engineering and Planning, Systems Development and Acquisition, Assessments, Joint Center for Global Connectivity, and Transformational Research & Development. These offices would be staffed jointly by appropriate agencies.

In FY 2006, the Domestic Nuclear Detection Office plans to:

- Develop the system architecture, conduct all associated systems engineering, develop technology roadmaps, and develop a strategic plan for the DNDO.

- Define the domestic nuclear detection architecture.
- Conduct research and development in support of the DNDO mission.
- Coordinate with other Federal, state, and local R&D organizations.
- Develop concepts for innovative technologies and coordinate with interagency R&D organizations on all advanced detection technologies, development concepts, and programs.
- Develop and provide technical standards and protocols for detection systems, reporting systems, and information sharing systems.
- Design and conduct technical and operational test and evaluation of related detection equipment, technologies, systems, procedures, concepts of operation, and protocols for the domestic nuclear detection system.
- Prepare and maintain the DNDO Test and Evaluation Master Plan.
- Oversee the Radiological and Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC) and use other Rad/Nuc test infrastructure as needed to execute the Office's assessment responsibilities.
- Provide operational support, to include: (1) information collection, coordination, and analysis; (2) coordinated technical reachback; and (3) and the development of standards, protocols, concepts of operations, training, safety and security procedures, and state and local support.
- Identify technology opportunities and execute programs to dramatically improve the domestic nuclear detection system overall and component-wise performance, especially high-risk, high-payoff technology investments.

Threat and Vulnerability, Testing and Assessment

Our Threat and Vulnerability, Testing and Assessment (TVTA) portfolio is designed to develop, test, and deliver – in collaboration with intelligence, law enforcement, and homeland security community agencies – tools and methodologies for assessing terrorist threats and understanding terrorism. The TVTA portfolio focuses on the following five areas:

- Threat Assessment: Create and establish coherent capabilities for analysis, dissemination, visualization, insight, synthesis, and enhancement of terrorism-related information
- Data Sharing: Enable tactical and strategic sharing of terrorism-related intelligence, information, and data among all elements of the homeland security community
- Forecasting: Identify, understand, and forecast terrorist motives, intentions, behaviors, capabilities, processes, and tactics; understand individual and societal resilience to terrorism
- Scalable Analyses: Enable scalable, integrated simulation and information analyses for threat identification and assessment; develop innovative computational technologies for deployment in next-generation knowledge management and threat assessment tools
- System Optimization: Create optimized knowledge system designs and architectures that enhance the nation's countermeasures

This portfolio provides the science and technology needed to develop methods and tools to test and assess threats and vulnerabilities to protect critical infrastructure and enhance information exchange; this portfolio also includes a Biometrics Program.

In FY 2004 and FY 2005, the TVTA Countermeasures portfolio:

- Delivered two operational components, the Threat Vulnerability Integration System (TVIS) and the Threat-Vulnerability Mapper (TVM), to the Information Analysis and Infrastructure Protection (IAIP) Directorate. The TVM provides counterterrorism analysts with a simple, straightforward way to depict the geographic distribution of threats across the U.S. and to search the underlying databases for information on terrorists and attacks. TVIS integrates high-volume information analysis capabilities with specialized visualization tools that enable analysts to process large amounts of disparate intelligence data.
- Created the knowledge management architecture, known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) to integrate the various information analysis and synthesis, visualization, and knowledge discovery component capabilities. ADVISE will incorporate a comprehensive encyclopedia of chemical, biological, radiological, nuclear and explosive (CBRNE) threat and effects data. Pilot ADVISE systems for the BTS Directorate will be installed in FY 2005. Update the initial TVIS system at the Biodefense Knowledge Center with the enhanced ADVISE capability.
- Created the Interagency Center for Applied Homeland Security Technology (ICAHST) capable of addressing the technical needs of the Department and other members of the Homeland Security community. The center and its interconnected laboratories provides detailed technical information and guides research, strategy, and systems design for the broad range of technologies and techniques necessary to identify, understand, and remediate CBRNE threats.
- Completed an initial set of 120 all-CBRNE capability assessments for 20 terrorist organizations on the five CBRNE plus cyber threat agents. Continued support to the Nuclear Assessment Program (NAP) that judges the credibility of communicated nuclear threats for such clients as the FBI, DOE, and Department of State (DOS). In FY2005, continue to produce all-CBRNE capability assessments. An additional 20 terrorist groups' capabilities and intentions will be analyzed using information from the intelligence community.
- Continued to implement the capability to analyze terrorist threats and stimulate analytical insight using visualization tools and techniques in FY 2005. The National Visualization and Analytics Center (NVAC), established in FY2004, will produce a national agenda for visual analytics with broad input and support from the government, national laboratories and universities. The four NVAC core functions include research and development, education, technology evaluation and implementation, integration and coordination. Three Regional Visual Analytics Centers (RVACs) will also be established, to implement the visualization agenda on a regional scale. The RVACs will incorporate university research activities as well as commercial and other government visual analytics research into the national lab-oriented work of the NVAC.
- Established an integrated, national capability, called the Institute for Discrete Sciences (IDS), to investigate and develop the specialized computing algorithms and hardware architectures necessary to analyze massive amounts of diverse data from multiple, disparate, distributed data sources, and to model terrorist attacks and simulate

consequences on a real-time, high-resolution basis. Like the NVAC, the IDS will have broad interaction and support from the government, national laboratories and universities.

- Completed an engineering design for the Enhanced International Travel Security (EITS) system, initiated in FY 2004, which will enable several pilots to be implemented with the United Kingdom, Canada, and Australia. EITS allows the validity of travel documents and the identity of travelers to be determined in real-time at U.S. borders and other points of entry.
- Provided the science and technology needed in the development of biometrics for precise identification of individuals, and develop prototype instrumentation to aid authorized officials in detecting individuals with potentially hostile intent.
- Enabled a comprehensive capability for determining terrorist motivations, based on social, behavioral, and economic factors. Integrate this with techniques for determining terrorist or hostile intent as well as detecting deception.

In FY 2006, the Threat and Vulnerability, Testing and Assessment portfolio plans to:

- Enable the development of analytic resources and technologies to characterize terrorist capabilities, detect their activities, predict their intentions based on infrastructure vulnerabilities, strengthen preventive measures, and increase the ability to respond.
- Provide an enhanced, integrated capability for information synthesis, relying on a foundation of advanced semantic processing and visual analytics and supported by specialized discrete mathematics techniques and technology. This will provide comprehensive knowledge discovery and dissemination capabilities to a diverse set of users – from first responders to intelligence analysts.
- Develop a capability for information extraction, pattern discovery, group detection, and visualization for unstructured text as well as audio and video information to complement the existing capability for structured data.
- Continue expanding the roles of the NVAC and IDS by providing integrated capabilities to multiple DHS components, setting national agendas in visual analytics and discrete sciences, and furthering interagency cooperation.
- Create a National Homeland Security Support System (NH3S) using the ADVISE architecture and providing quantitative risk analysis and decision support capabilities.
- Create a CBRNE threat encyclopedia and integrate with the ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) system. Create a National Homeland Security Support System (NH3S) using the ADVISE architecture and providing quantitative risk analysis and decision support capabilities.

Standards Program

Ensuring that standards are created and adopted is critically important for homeland security. We need consistent and verifiable measures of effectiveness in terms of basic functionality, appropriateness and adequacy for the task, interoperability, efficiency, and sustainability. Standards will improve the quality and usefulness of homeland security systems and technologies. Our Standards Program cuts across all aspects of the S&T Directorate's mission and all threats to improve effectiveness, efficiency, and interoperability of the systems and technologies developed.

Our Standards Program continues to actively engage the Federal, state, and local first responders to ensure that developed standards are effective in detection, prevention, response, management, and attribution. This program office also conducts the essential activities in order to meet the requirement of the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act in developing certification standards for technologies related to homeland security.

In FY 2004 and FY 2005, the Standards Program:

- Composed three management directives to establish DHS policy with regards to the adoption and development of national standards.
- Formed an interagency task force to address the controversy over the effectiveness and use of lateral flow immunoassays for the detection of *Bacillus anthracis* (anthrax) by emergency responders.
- Evaluated a five step method to pre-screen suspicious white powders through an effort with Edgewood Chemical Biological Center (ECBC) and an additional effort with the National Institute of Standards and Technology (NIST) to look at the effectiveness of biological agent simulants, and the establishment of a program to address both chemical and biological decontamination standards for the first responder community.
- Supported efforts with American Society for Testing and Materials (ASTM) to coordinate the development of a draft standard for hospital preparedness and to develop a multi-disciplinary Mission Essential Task List (METL) based on Emergency Responder Guidelines developed by the Office of Domestic Preparedness.
- Within Standards for Personal Protective and Operational equipment, the program supported the development of a number of respiratory standards including three National Institute for Occupation Safety and Health (NIOSH) standards and one National Fire Protection Association (NFPA) standard adopted by DHS in February 2004.

In FY 2006, the Standards Program plans to:

- Continue to maintain and improve the process by which homeland security standards are developed and promulgated at the Federal level. Incorporate the appropriate conformity assessment program development into the standards development process. Maintain and update the homeland security standards database available to the homeland security community.
- Continue to utilize interagency working groups to reevaluate requirements and prioritize needs for CBRNE countermeasures standards. Focus on developing sampling protocols and guidelines and standardized sample triage methods for CBRNE countermeasures. Focus on standards for emerging CBRNE countermeasures technologies including CBRNE point detectors; CBRNE stand off detectors and urban surveillance technologies such as BioWatch, CBRNE facility monitors, and water distribution monitors. Continue programs to address multimodal biometrics, latent fingerprints, rapid biometric evaluations, and biometric image and feature quality. Also explore and evaluate ergonomics, human factors, and usability issues of biometric sensors, software, and systems.

- Continue with the completion of a standard guide for building event dispersion and health assessment preparedness and response planning and the standard guide for conducting emergency preparedness drills and exercises.
- Continue current CBRNE personal protective and operational equipment specifically focusing on completing the suite of respiratory protection equipment standards to include powered air purifying respirators, closed-circuit self contained breathing apparatus, supplied air respirators and combination respirators.

Support to Department of Homeland Security Components

As I have mentioned, the operational components of the Department are my customers. To ensure we meet customer needs, the S&T Directorate has established the Science and Technology Requirements Council (SRC) to bring forward a set of vetted needs from the entire Department. This is an Assistant Secretary level committee with representation from across DHS that has been chartered to assist in the solicitation, validation, and prioritization of all science and technology requirements. This council is intended to help the S&T Directorate identify those needs most crucial to the DHS mission and to develop the most effective S&T program possible using existing resources. As part of their mission, the SRC reviews DHS operational requirements and needed capabilities that require S&T solutions, and identifies those opportunities that have cross-cutting technology solutions. Prioritized Departmental needs are then presented to me as a recommendation for consideration, in conjunction with all externally derived S&T requirements (e.g., statutory, national guidance), for inclusion in the S&T Directorate's Planning, Programming, and Budgeting Cycle Guidance.

The inaugural meeting of the SRC took place September 30, 2004, and was attended by representatives from Border and Transportation Security (BTS), Emergency Preparedness and Response (EP&R), Information Analysis and Infrastructure Protection (IAIP), the Office of Domestic Preparedness (ODP), U.S. Citizenship and Immigration Service (CIS), U.S. Coast Guard (USCG) and U.S. Secret Service (USSS). Our initial meeting resulted in new requirements and a validation of the needs that our portfolios had already identified through their interactions with the rest of the Department. It further served to bring together the many disparate groups from across DHS and facilitated a new dialogue that will be necessary to produce a successful S&T RDT&E program. The input we received at the September 30, 2004, meeting was used to adjust the FY 2006 budget request and is currently being integrated into our FY 2007-2011 Planning, Programming and Budgeting cycle.

I will now address the specific programs being conducted by our mission support portfolios.

Support to Border and Transportation Security

The Science and Technology Directorate supports all elements of BTS enforcement and facilitation processes through identifying operational requirements, developing mission capabilities-based technological needs, and implementing a strategic plan. We are providing systems engineering support to various BTS programs including US VISIT and Unmanned Aerial Vehicles.

The Science and Technology Directorate's support to the BTS Directorate is accomplished by implementing a capabilities-based technology planning process. The capabilities-based approach establishes the scope of effort and framework for a technology plan. Through a series of user conferences and technology opportunity conferences, requirements are developed and prioritized for new and improved capabilities. Operational personnel identify capabilities and technology personnel identify potential development opportunities. Capability gaps and possible technology solutions are proposed, and a budget is developed to distinguish between both funded and unfunded needs.

The Science & Technology Directorate, in collaboration with BTS, co-chairs the Department's Unmanned Aerial Vehicle (UAV) Working Group. This group is currently focused on developing the Border and Transportation Security operational requirements for UAVs and related technologies, e.g., aerostats, blimps, lighter than air (LTA) ships, and fixed and mobile towers. The UAV Working Group has identified the following six BTS capability objectives that could benefit from the utilization of UAVs:

- surveillance and monitoring
- communications
- apprehension
- targeting
- intelligence
- deterrence
- officer safety

Based on these high-level requirements, the Science and Technology Directorate is developing concepts of operations and assumptions that will be used in conducting an Analysis of Alternatives that will include UAVs as well as other technologies.

- Over the past two years, the Science & Technology Directorate has sponsored two major evaluations of Unmanned Aerial Vehicle (UAV) technology as part of the Arizona Border Control Initiative.

In FY 2004 and FY 2005, the Border and Transportation Security R&D portfolio:

- Issued a solicitation for an Advanced Container Security Device to develop and field test (within the Directorate's CounterMeasures Test Bed) the next generation of shipping container security devices, building on the current efforts through Operation Safe Commerce as well as current Border and Transportation Security policy efforts to develop and implement performance requirements for container security. The Advanced Container Security Device program is part of a "Future Smart Container" initiative encompassing container security, communications, and data systems for the future.
- Supported the BTS Directorate in putting technology in the field to support the Arizona Border Control Initiative. The portfolio demonstrated other technologies such as a long-range acoustic device that allows agents to communicate from a safer standoff distance to determine the intent of people.
- Continued development and refinement of BTS technology requirements and planning. Using a capabilities-based process, the portfolio's goal was to ensure that Federal

technology planners understood the capabilities that BTS agents and officers view as essential for mission success and to help planners focus technology development on filling the identified gaps in those capabilities.
- Developed the BTS Technology Vision which include Border Watch, Transportation Watch and Border Net which significantly improves our ability to provide the information necessary to secure our borders. The foundation of the vision is an architecture and a set of technology programs that will gather, process and distribute real-time knowledge of the border and transportation situation and provide decision support tools and labor saving devices for our security forces.

In FY 2006, the Border and Transportation Security R&D portfolio plans to:

- Build on the sensor trade studies and modeling conducted in FY 2005 to develop and test advanced sensor suites including improved visual and non-visual sensors (video, infrared, seismic, acoustic and radar). These sensors may be deployed on the ground, at sea, and in the air. In addition, evaluate data produced by Ports-of-Entry (POE) inspectors, such as traffic and incident information, along with data produced by border inspection systems will be evaluated as part of the surveillance system.
- Build on the design and development effort accomplished in FY 2005 on the next generation of container security and communications systems to detect intrusion, location, contents and tampering. The requirements for this system include recording and reporting location; detection of intrusion and communication of log history, and sensor and inspection data.
- Integrate Transportation Watch capabilities across the transportation domains enabling a Common Operational Picture (COP) across the entire transportation environment. Extensive data sharing, including the ability to discover links in criminal or suspicious activities across domains will be a key requirement to providing an effective Transportation COP.
- Initiate development and integration of smart portals and sensors for detection of explosive threats to shipping. Utilize rapid prototyping processes, focusing initially on passenger and vehicle ferries.
- Define system architecture that fully supports the Border Watch Common Operational Picture with multi-modal access to essential databases, remote communications and intelligence fusion.

Support to Emergency Preparedness and Response

The S&T Directorate's Emergency Preparedness and Response (EP&R) portfolio supports the Department's EP&R Directorate with a mission to improve the ability of the nation to prepare for, respond to, and recover from all-hazards emergencies through development and deployment of enabling capabilities. Particular emphasis is placed on technology integration at all levels of government, detection and monitoring systems for chemical, biological, radiological, nuclear and explosive (CBRNE) threats, and long-term sustained performance and interoperability enhancement of state and local preparedness. The most important customers of EP&R technologies are the Federal, state and local emergency responders and emergency managers

who are first into an emergency zone and often last to leave. Specific objectives of the portfolio are to:

- Identify and develop relevant technology solutions through partnerships with operational end-users;
- Integrate advance all-hazards technology into Federal, state, and local emergency response infrastructures; and
- Provide scientific and technology leadership for implementation of HSPD-5 (Management of Domestic Incidents) and HSPD-8 (National Preparedness) efforts

In FY 2004 and FY 2005, the Emergency Preparedness and Response R&D portfolio:

- Initiated operation of the Interagency Modeling and Atmospheric Assessment Center (IMAAC) and supported the National Exercise Program and special events, such as the Democratic and Republican National Conventions. IMAAC established connectivity to the Department of Homeland Security Operations Center and the FEMA National Emergency Operations Center to provide near real time hazards predictions for airborne releases.
- Selected four urban areas for the pilot of the Regional Technology Integration (RTI) Initiative. These locations provide an opportunity to evaluate geographic and governance diversity as well as variability in threats and vulnerabilities. Initiated an integrated assessment process in collaboration with these communities.
- Focused activities on the identification of simulation based training and education requirements through interaction with the responder community. The portfolio leveraged the work initiated by Office of Domestic Preparedness and the Memorial Institute for the Prevention of Terrorism, the National Institute of Justice and the Department of Defense in identifying needs and gaps as well as existing technology development programs that can be utilized for incident management training

In FY 2006, the Emergency Preparedness and Response R&D portfolio plans to:

- Leverage Federal resources to provide dynamic venue for collaborative research, development, testing and evaluation of atmospheric transport and dispersion (ATD) models for hazards predictions. IMAAC will host researchers from throughout the nation at its facility as well as participate in virtual collaboration both nationally and internationally.
- Complete implementation of technology systems solutions for the first four pilot locations of the RTI initiative; prepare test and evaluation plans and conduct operational readiness exercises to evaluate the overall system performance.
- Develop the system requirements that support national, interoperable simulation based training and exercise. This capability will focus on large scale, multi-jurisdictional incidents and will facilitate the implementation of the National Incident Management System and the National Preparedness Goal.
- Demonstrate several revolutionary and highly innovative materials for emergency personal protective equipment (PPE) applications. Demonstrate prototype

material/technologies that can that can be made into functional garments and/or integrated personal protective systems will be demonstrated.
- Initiate an Advanced Concept Technology Demonstration of a candidate Unified Incident Command (UIC) architecture that will achieve revolutionary advances in Unified Incident Command and Decision Support and bring analytical tools to bear on real-time information in-flows and out-flows for incident commanders and emergency responders. Advanced capability will be applicable to a variety of response paradigms, including single incidents, multiple simultaneous incidents, long duration response and recovery operations, and large-scale public health events.

Support to United States Coast Guard

The mission of the United States Coast Guard (USCG) R&D portfolio is to develop technology and systems to provide the capability to safeguard lives, property and environment from intentional and accidental maritime threats and protect maritime mobility through the free flow of goods and people while maximizing the recreational use of the Nation's waterways.

The USCG R&D portfolio covers the Homeland Security (HLS) and Non-HLS missions performed by Coast Guard operational forces. HLS priorities include research programs that address a defense in depth, or layered approach, to Maritime Domain Awareness, Prevention/Protection, Response and the management, analysis and distribution of information, (e.g., Sea Guardian, Coastal Shield, Port Protector and Smart Commander). Similarly, USCG non-HLS mission research needs (e.g., Search & Rescue, Maritime Oil Spill Response, Aquatic Nuisance Species, Waterways Navigation, etc.) are addressed through programs like Safe Voyage, Clean Sweep, ANS Eradicator and Able Navigator. Together these programs support the five Strategic Goals of the USCG (Maritime Safety, Protection of Natural Resources, Maritime Security, National Defense, and Maritime Mobility).

The USCG portfolio expects in FY 2006 to see the continuation of HLS mission research in the following areas:

- Situational Awareness for Maritime Domain Awareness – develop automated classification and prediction capability for vessel intent with a port area.
- Compel Compliance – field new capability to communicate and stop at-sea small prop-driven vessels and in port swimmers/divers.
- Boarding Capability – improve space accountability for non-ferrous vessels.
- Personnel Alerting and Contraband Detection and Identification – adapt breakthrough. Technologies in CBRNE countermeasures for the maritime environment.

For non-HLS mission support, this portfolio will continue to place its highest priorities on high-risk, high-reward research and development relevant to the Coast Guard's traditional mission set that might not otherwise be addressed in order to enhance operational components within the Coast Guard. Non-HLS mission support will address Coast Guard Strategic Goals (i.e., Maritime Safety, Security and Mobility, and Protection of Natural Resources) through RDT&E efforts that will provide increased knowledge, capability and performance improvements in the following areas:

- *Aquatic Nuisance Species Eradication*: non-invasive treatment of ballast water;
- *Oil Spill Detection & Response*: fielding of new technology, equipment and devices to detect subsurface and submerged *(heavy)* oils from standoff distances;
- *Rapid Hazardous Material (HAZMAT) Response Information*: evaluate airborne detection capability for heavy oil spills and identify Commercial-off-the-Shelf (COTS) technologies for HAZMAT identification by USCG inspection personnel; and
- *Search & Rescue*: incorporate environmental/meteorological data into CODAR improving current analysis and short term forecasting for target movement and search area predictions; develop improved Last Known Position estimators in support of USCG Search Area Planners resulting in reduced search areas and increasing survivability of persons lost at sea.

Support to the United States Secret Service

The mission of the United States Secret Service (USSS) portfolio of the S&T Directorate is intended to support the unique USSS mission by development and deployment of advanced technologies to enhance protective and investigative capabilities. This portfolio is coordinated with the United States Secret Service and has established its first direct-funded R&D program. The USSS portfolio effort focuses upon input from the intelligence community (threat based model) and direct operational experience obtained over the last century. As a result, this funded technology program is subject to reevaluation and change based upon the perceived threats to the safety of those protected by the USSS.

In 2004, the portfolio addressed four projects/programs. The Emerging Threats Program supports the Secret Service's continuing, comprehensive assessments of emerging threats and evolving technologies that pose a threat to dignitaries and assets protected by USSS personnel. The Law Enforcement Virtual-Reality Training Model program supports prototyping and deployment of a law enforcement security-oriented simulation training system for the USSS-specific training and modeling. Additionally, this system will enhance the effectiveness of emergency responders during actual events. The Critical Structure Protective Initiative (CSPI) program will ensure continued research and development of network protection systems and procedures designed to mitigate exploitation of site-specific "Very Large Scale Integration" (VLSI) control architectures. The Wireless Tracking Device program supports development of a handheld, man-portable wireless tracking device for locating operators of wireless communication device(s) in difficult radio frequency environments such as an office building or event stadium.

In FY 2006, the U.S. Secret Service Portfolio plans to continue development of appropriate escape hood technology, begin the development of a mobile platform that will be required to detect, exploit, and defend against covert and overt electronic surveillance systems, continue (given a successful proof of concept in FY 2005) with the development of a ubiquitous mobile computing system that would allow secure wireless networked communication between unlike devices with high fidelity data transmission; and initiate an Optical & Chemical Tagging/Tracking Project under this program**.** This project's objective will be the development of optical and chemical tags that are robust and covertly deployable.

Homeland Security University and Fellowship Programs

In this portfolio we seek to develop a broad research capability within the nation's universities to address scientific and technological issues related to homeland security. The portfolio places a high priority on developing academic programs and supporting students in order to build learning and research environments in key areas of Departmental interest.

In FY 2004, the Homeland Security University Programs established three Centers of Excellence:

- The Center for Risk and Economic Analysis of Terrorism Events, at the University of Southern California and its partners will receive $12 million over three years to evaluate the risks, costs and consequences of terrorism and to guide economically viable investments in countermeasures.

- The National Center for Foreign Animal and Zoonotic Disease Defense at Texas A&M and its partners will receive $18 million over three years to address potential threats to animal agriculture including Foot and Mouth Disease, Rift Valley fever, Avian influenza and Brucellosis. In addition to working closely with industry and government, they will work with DHS's Plum Island Animal Disease Center.

- The National Center for Food Protection and Defense at the University of Minnesota and its partners will receive $15 million over three years to establish best practices and attract new researchers to manage and respond to food contamination events, both intentional and naturally occurring.

In FY 2005, DHS announced the selection of the University of Maryland (UMD) and its partners as the Center for Behavioral and Social Research on Terrorism and Counter-Terrorism. This Center will be funded at $12 million for three years following contract award

During late FY 2005 and early FY 2006, the S&T Directorate expects to establish at least three additional Centers of Excellence. Each Center is awarded an initial three-year grant whose annual cost we account for in our planning.

As part of the Department's mission to maximize collaboration with other Federal agencies, University Programs and EPA's Science to Achieve Results (STAR) Program have collaborated on the topic of microbial risk assessment. The DHS-EPA cooperative Center on Microbial Risk Assessment will result in one five-year grant to a university-based consortium will be jointly funded by both agencies for a total of $10 million.

Last fall, University Programs selected approximately100 students for the 2004 class of DHS Scholars and Fellows bringing the total of students to about 200. Students from the 2003 and 2004 class participated in a DHS orientation for the purpose of learning about DHS mission objectives, the critical research needs, and meeting scientists from DHS laboratories, Centers of Excellence and DOE national laboratories. Students from both classes are attending 93

institutions (including Historically Black Colleges and Universities/Minority Serving Institutions) in 38 states and the District of Columbia. Seventeen of the institutions are located in Experimental Program to Stimulate Competitive Research (EPSCoR) states. Besides making immediate contributions to homeland security-related R&D, these students will be part of the development of a broad research capability within the Nation's universities to address scientific and technological issues related to homeland security.

Beginning in FY 2006, the steady state of up to 300 highly talented and diverse students will be maintained.

Emerging Threats

It is truly the threats we do not yet know that are often the most terrifying. Our Emerging Threats portfolio addresses the dynamic nature of terrorist threats, as science and technology advancements enable new agents of harm and new ways to employ them. This portfolio places high priority on developing the capability to use innovative, crosscutting, out-of-the-box approaches for anticipating and responding to new and emerging threats. Successful identification of emerging threats will permit capabilities to be developed to thwart these emerging threats before they are used.

Relevant R&D is underway at other agencies and organizations; thus, partnerships in this area hold great potential for synergistic focus on homeland security. Work is being done and will continue to be pursued in partnership with the Departments of Energy, Defense, Justice, and Agriculture, the intelligence community, and the National Institutes of Health.

In FY 2004 and 2005, the Emerging Threats portfolio:

- Established informal partnerships with the intelligence community and with the USSS portfolio to leverage ongoing activities in support of over-the-horizon assessment.
- Initiated efforts, in combination with Rapid Prototyping, in both near-term and breakthrough solutions to homeland security issues. Near-term projects are funded out of the Rapid Prototyping Portfolio. Breakthrough projects are funded from the Emerging Threats Portfolio.
- Held a privacy protection workshop in which the technical and policy communities interacted to identify important technical challenges and high impact solution areas. Information from this workshop will form the basis of upcoming programs in this area.
- Analyzed multiple radar technologies and other surveillance strategies to determine which combination of technologies would best support coastal surveillance by the USCG.
- Conducted three sensitive projects, two in collaboration with the USSS and one addressing a critical infrastructure.
- Sponsored studies at the Homeland Security Institute to identify threat and technology trends and develop a framework for analyzing emerging and future threats to homeland security.

In FY 2006, the Emerging Threats portfolio plans to:

- Sponsor comprehensive assessments to identify and prioritize emerging threats. The outcomes of the assessments lead the strategic programs to integrate multiple disciplines and threat scenarios and comprehensively use intelligence-based information to establish organizational foresight.
- Fund research dedicated to long-term, undefined threats as a means to exercise technology influence in the marketplace and build infrastructure to incentivize non-requirements driven, high-risk, high-payoff R&D, thereby promoting technology push and collaboration to solve otherwise intractable problems.
- Complete development of projects initiated in FY 2005, and test and evaluate the products from these projects. Develop technologies and systems against emerging threats identified as a result of FY 2005 emerging threats analysis.

Rapid Prototyping

By accelerating the time needed to develop and commercialize relevant technologies, the Science and Technology Directorate will ensure that operational end-users will be better able to prevent terrorist attacks, reduce the nation's vulnerability, and minimize the damage and assist in recovery if attacks occur. Our Rapid Prototyping portfolio advances the Directorate's mission to conduct, stimulate and enable RDT&E and timely transition of homeland security capabilities to Federal, state and local operational end-users.

In FY 2004 and FY 2005, the Rapid Prototyping portfolio:

- Solicited ideas, concepts and technologies for 50 requirement areas of interest to both the Department and other agencies. Initiated efforts to address chemical and biological threats, explosive detection, training technology tools, improvised nuclear device defeat, and investigative and forensic support topics.
- Developed a joint port and coastal surveillance prototype designated HAWKEYE with the United States Coast Guard (USCG) that provides an integrated maritime surveillance system covering Port Everglades, Miami, and Key West, Florida. This first-of-its-kind integrated command center and maritime surveillance facility opened in July 2004.
- Initiated the implementation of the Technology Clearinghouse as required in the Homeland Security Act of 2002. This clearinghouse serves as the central nexus to the public safety and first responder community on: (1) Information services supporting access to, and dissemination of, information regarding innovative technologies serving the DHS mission; (2) Resources designed to support the collaborative needs of teams serving the mission of DHS; and (3) Technology programs and resources themselves, designed to serve the mission of DHS and distributed via a central DHS mechanism.

In FY 2006, the Rapid Prototyping portfolio plans to:

- Transition mature programs from the development phase to operational testing and evaluation programs and commercial or government entities for deployment. Identify new technology candidates and capabilities to meet the existing and emergent technical requirements of the Department.

- Continue support of the Technology Clearinghouse in FY 2006 and continue to fund projects initiated under the Near Term and Future Technologies solicitation released in FY 2004.
- Complete the development of projects, within the Support to State and Local Responders project, initiated in FY 2005, and test and evaluate the products from these projects.

Counter-MANPADS

The Counter-MANPADS program is focused on demonstrating the viability, economic costs, and effectiveness of adapting existing military technology to protect commercial aircraft from the threat of Man Portable Air Defense Systems (MANPADS). The major thrust of this program is to demonstrate and evaluate the possible migration of existing technologies to the commercial airline industry, not to develop new technologies. The resulting countermeasure systems must have minimal impact on air carrier and airport operations, maintenance, and support activities. The re-engineering of existing countermeasure technologies and components is necessary to meet commercial air carrier operation requirements, including protection of critical military technology. The program balances cost, schedule, and performance with the needs and requirements of the aviation community stakeholders. Upon completion of a two-phase analysis, prototype and testing program, DHS will provide the Administration and Congress with a recommendation for the most viable solution to defend against shoulder-fired missiles.

To mature the reliability of the underlying military technology to commercial standards, validate system effectiveness and suitability in an operational environment, and to develop and implement a comprehensive approach to technology protection, a follow-on Phase III has been planned. Phase III will include delivery and installation of pre-production Counter-MANPADS equipment on commercially operated aircraft by U.S. cargo carriers similar to those aircraft dedicated to meet Civil Reserve Air Fleet (CRAF) requirements. This will integrate a limited number of systems on multiple airframes in actual revenue service across the different carriers for the purpose of operational testing and evaluation, data collection, and the certification of a number of different aircraft types. Phase III remains subject to approval by the Administration and Congress.

In FY 2004 and FY 2005, the Counter-MANPADS program:

- Initiated and completed Phase I following a competitive bidding process. DHS awarded Other Transaction (OT) for Prototype Agreements (OTA) to three companies - BAE Systems, Northrop Grumman, and United Airlines - for Phase I of a two-year System Development and Demonstration (SD&D) effort. The contractors focused on proving the feasibility of migrating existing DoD technology into the commercial sector and exploring other technology as appropriate. Following Preliminary Design Reviews with all three companies in July 2004, the Phase I portion of the twenty-four month SD&D effort concluded and DHS initiated a selection evaluation process to determine which of the three companies would be selected to further mature their preliminary designs, build representative prototypes, install them on aircraft, and conduct formal testing during the Phase II eighteen month effort.
- Involved the stakeholder community beginning in FY 2004. In late 2004, the Program

Office hosted a Stakeholders' Meeting, attended by representatives of the airlines, the equipment manufacturers, and other affected sectors, including representatives of multiple Federal government Departments and Agencies.

In FY 2006, the Counter-MANPADS program plans to:

- Build, deliver, install, and fly pre-production counter-MANPADS equipment on commercially-operated aircraft by US cargo carriers similar to those aircraft used for the Civil Reserve Air Fleet (CRAF) operations.
- Conduct operational testing and evaluation and data collection on multiple aircraft types to capture operational and maintenance costs as well as technical performance and reliability data in a commercial operational environment.
- Modify Phase II systems to incorporate new design requirements including reliability, technology protection, and emergency ground notification improvements based on test and evaluation results.
- Examine maintaining two contractors in Phase III to foster competition, and to promote manufacturing should a full-rate decision be made.
- Conduct an aggressive reliability growth effort to increase system reliability to 3000 hours and reduce recurring support costs.
- During CY 2006, conduct Live-Fire Test and Evaluation assessment
- Continue on-going dialogues with Original Equipment Manufacturers (OEM) such as Boeing and Airbus and conduct studies to scope the effort required to include provisions for Counter-MANPADS systems on future production aircraft.
- Pursue Federal Aviation Administration certification for additional aircraft types/models/series not addressed in Phase II.

Office of SAFETY Act Implementation

The mission of the Office of SAFETY Act Implementation (OSAI) is to evaluate technologies submitted to it by applicants in accordance with the criteria set forth in the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) and Interim Regulations. As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY Act to provide "risk management" and "litigation management" protections for sellers of qualified anti-terrorism technologies. The purpose of the Act is to encourage the development and deployment of anti-terrorism technologies (ATT) that will substantially enhance the protection of the nation. Specifically, the SAFETY Act creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified anti-terrorism technologies have been deployed.

Although there are many technologies that are important to protecting our homeland, the SAFETY Act Designation and Certification are designed to support effective technologies aimed at preventing, detecting, identifying, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause, and which also meet other prescribed criteria.

OSAI evaluations are designed to generate advice to the Under Secretary on the appropriateness of granting protections under the SAFETY Act. In support of this mission, OSAI undertakes

efforts to raise public awareness of the benefits of the protections available under the SAFETY Act. In addition, OSAI coordinates its process with other offices within DHS and other Federal agencies to both support those offices in their missions and to minimize the burden on applicants for SAFETY Act protections.

The Department moved quickly to create OSAI. In July 2003, a notice of proposed rulemaking was published for comment, and on October 16, 2003, an interim rule was published with a request for public comments, thus implementing the program. Facilities to house the program were selected and OSAI has identified and entered into agreements with the lead implementation contractor and lead web site development/management contactor. OSAI designed and implemented a web-based application kit and process with an interactive help desk. OSAI executed a robust outreach program to introduce the industry to the SAFETY Act program and to encourage its participation. OSAI has received and has responded to 72 full applications and 166 pre-applications. Four applicants have been awarded SAFETY Act designation and certification: Northrop Grumman; Michael Stapleton Associates; Teledyne Brown Engineering; and Lockheed Martin.

The Office intends to refine its operations throughout FY 2005. OSAI, in consultation with the Department's Office of the General Counsel, has been revising the Interim Rule based on the comments received from the public and our experiences with applicants over the past year. OSAI will revise the application kit to make it clearer and more user-friendly, and will work to streamline the process based on lessons learned from the previous year. The number of applications is expected to increase significantly with the introduction of the revised kit, implementation of the Final Rule, and higher visibility.

In FY 2006, OSAI plans to expand its coordination of the program with pending Federal, state, and local procurements. It also plans to work with recognized procurement organizations and appropriate industry associations to educate them on the availability of SAFETY Act protections to potential vendors.

Office of Interoperability and Compatibility

The Office of Interoperability and Compatibility (OIC), managed by the S&T Directorate, was tasked to lead the planning and implementation efforts in coordination with other DHS programs. It oversees the wide range of public safety interoperability programs and efforts currently spread across Homeland Security. These programs address critical interoperability issues relating to public safety and emergency response, including communications, equipment, training, and other areas as needs are identified.

Creating interoperability requires coordination and partnerships among managers, partners, and stakeholders at all levels of government. OIC will establish partnerships with all relevant offices and agencies to ensure that the programs address all possible issues related to public safety interoperability and compatibility. These partners and additional relevant stakeholders include representatives from the emergency response providers represented by their national associations, state and local government agencies, DHS and other Federal government agencies, standards development organizations, and industry.

Since October 2004, the OIC has interviewed key stakeholders across federal and practitioner communities to validate findings, uncover additional interoperability initiatives, and determine key issues for first response; identified a core group of federal programs that test and evaluate first responder equipment; began developing a plan to establish a Joint Evaluation and Testing Program to coordinate with other federal agencies; and conducted an initial scan of existing programs for first responders and collected information at the local, state, and federal levels.

Critical Infrastructure Protection Portfolio

The Science and Technology Directorate's Critical Infrastructure Protection (CIP) portfolio protects the nation's critical infrastructure and key assets from acts of terrorism, natural disasters, or other emergencies by developing and deploying tools to anticipate, identify and analyze risks, and systems to reduce those risks and the consequences of an event. The portfolio puts a focus on scientific prioritization of components of critical infrastructure and key resources/assets and partners with other organizations to catalyze development of critical infrastructure protection technologies.

In FY 2004 and FY 2005, the Critical Infrastructure Protection R&D portfolio:

- Developed a CIP Decision Support System (DSS) focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection. The prototype model includes representation of all 14 critical infrastructure sectors, as outlined in the National Strategy for the Protection of Critical Infrastructures and Key Assets, as well as their interdependencies. Preliminary test cases have been used to develop consequence estimation features of the CIP-DSS at both national and metropolitan scales.
- Initiated a system study to find potential solutions for personnel surety for security guards that guard our Nation's Critical Infrastructure, as well as insiders with access to sensitive areas of, or information about the infrastructure.
- Supported a System Study for Municipal Domestic Water Security, along with the Biological Countermeasures Portfolio, Chemical Countermeasures Portfolio, and Radiological/Nuclear Countermeasures Portfolio.
- Initiated interagency development of the first annual National Critical Infrastructure Protection R&D Plan using the Infrastructure Subcommittee of the National Science and Technology Council.
- Initiated cooperative and collaborative research and development project with the Kentucky Homeland Security University Consortium comprised of the University of Kentucky, the University of Louisville, Eastern Kentucky University, Western Kentucky University, Northern Kentucky University, Morehead State University, Murray State University, Kentucky State University and the Kentucky Community & Technical College System.

In FY 2006, the Critical Infrastructure Protection R&D portfolio plans to:

- Incorporate a fully parameterized metropolitan area modeling capability into the CIP-DSS. Integrate adversary-defender constraint and information dynamics models into CIP-DSS. Add an enhanced threat spectrum capability to CIP-DSS and complete pilot tests of the CIP-DSS in several state and regional areas.
- Publish the National Academy Study on Security of the Electrical Industry.
- Complete the quick-look system studies of all 14 Critical Infrastructures and Key Resources, and the end-to-end System Study for Municipal Domestic Water Security.
- Deliver improved closed circuit TV (CCTV) components for object identification and behavior recognition. Deliver an enhanced threat detection CCTV system based on video image understanding architecture, including the improved CCTV components.
- Deliver the second annual National CIP R&D Plan with agency budget information and a roadmap for deliverables. Incorporate relevant inputs from: a) federal agencies including activities, and levels of effort; b) critical infrastructure sector owners and operators; and c) private and public research institutions and universities.

Cyber Security R&D Portfolio

The Cyber Security R&D Portfolio supports the mission of the Information Analysis and Infrastructure Protection Directorate and is focused on leading cyber security research, development; testing and evaluation endeavors to secure the nation's critical information infrastructure through coordinated efforts that will improve the security of the existing cyber infrastructure, and provide a foundation for a more secure infrastructure. This will be accomplished by focusing on R&D aimed at preventing, protecting against, detecting, responding to, and recovering from large-scale, high-impact cyber attacks, supporting the development and accelerating the deployment and use of more secure Internet communication protocols, addressing cyber security R&D needs that are unique to critical infrastructure sectors, and provide novel and next-generation secure information technology concepts and architectures.

In FY 2004 and FY 2005, the Cyber Security R&D portfolio:

- Initiated dialog aimed at international collaboration on cyber security R&D with Canada, the United Kingdom, and Japan. Interactions with the United Kingdom and Japan are at early stages and have not yet reached the point where potential joint R&D activities have been identified.
- Worked with Federal researchers and officials and the private sector to develop a roadmap to accelerate the development and deployment of a secure domain name infrastructure. Current work also includes the identification of technology requirements and development of models to aid in assessing the performance impact of utilizing Domain Name System Security Extensions (DNSSEC) in operational environments.
- Initiated a program to address different facets of the need for improved methods for cyber security assessment and testing, in order to provide a foundation for the long term goal of economically-informed risk-based cyber security decision making.
- Provide technical support funding through the “virtual” Cyber Security R&D Center for the S&T Directorate in pre-research activities (such as developing roadmaps, organizing workshops and meetings, aiding in drafting research solicitations and proposal review), as well as post-research activities (such as facilitating pilot tests and exercises, venture

capital community outreach, private sector outreach, and interfacing with non-government R&D communities).

In FY 2006, the Cyber Security portfolio plans to:

- Continue to provide support to the Directorate through the "virtual" Cyber Security R&D Center in pre-research activities and post-research activities. FY 2006 activities will have a significant focus on private sector and venture capital community outreach.
- Initiate a new two-year R&D program phase, again overlapping with the program started in FY 2005. As the FY 2004 program comes to a close in FY 2006, progress against the FY 2004 technical topic areas will be evaluated.
- Complete full-scale operational test bed, acquisition and generation of network data sets, enhancement of remote management and configuration capabilities, and a final project report.
- Focus on system-level DNSSEC implementation, with the development of software reference implementations for servers and client applications, and planning for pilot deployments of DNSSEC. Direct investments in the area of routing protocol security at the development of a modeling and simulation framework for impact assessment of secure routing protocols on the Internet performance.
- Focus on pursuing partnerships that allow broader non-government participation, accompanied by a greater role of non-government organizations and funding sharing responsibility for oversight and financial support for this capability.

R&D Consolidation

Funds originally requested by the U.S. Coast Guard to support operations, maintenance and salaries for the assigned science staff for the Coast Guard Research and Development Center will be integrated into the Science and Technology Directorate mission space to support the continued operations and scientific activities at the Coast Guard Research and Development Center. Funds originally requested by the Customs and Border Protection (CBP) to support salaries for those assigned to the Research, Development, and Evaluation Branch will likewise be integrated into the S&T Directorate mission

In FY 2006, DHS's Science and Technology Directorate will unite the RDT&E functions of the existing S&T explosives countermeasures portfolio along with those of the Transportation Security Administration program. The resulting integrated portfolio will then encompass and support the true objective of the explosives countermeasures technology program: to prevent, detect, respond, and mitigate the use of explosives in attacks against the population, mass transit, civil aviation, critical infrastructure and key assets. This consolidation allows for an expansion of the scope and number of programs within the explosives countermeasures portfolio in comparison to the current FY 2004 and FY 2005 and planned FY 2006 activities. Programs include explosives marking, smuggling, aviation security, suicide bomb interdiction, and vehicle bomb interdiction.

FY 2006 Science and Technology Directorate Initiatives

The S&T budget request includes funding for a number of mission-critical initiatives.

- **National Bio and Agrodefense Facility.....$23 million**
  The National Bio and Agrodefense Facility (NBAF) will extend the capabilities of the National Biodefense Analysis and Countermeasures Center (NBACC) for threat characterization, forensics, and detection to defend both animal and public health. Research, development, test and evaluation at the NBAF will strengthen the nation's ability to anticipate, prevent, respond to, and recover from the intentional introduction of high consequence biological threats, such as Foreign Animal Diseases. The S&T Directorate will focus on developing and testing the technical means to prevent attacks on agriculture and humans and strengthening the capability to respond to an attack, recover from an attack, reconstitute the agricultural economy and infrastructure, and provide a means to identify the bioterrorists and bring them to justice. The NBAF will enhance situational awareness of the health of the American populace, animals, plants, food supply, and environment, and result in better informed decision making and a quicker Federal, state, and local response to foreign animal and zoonotic diseases. The capabilities provided by the NBAF meet the requirements of HSPD-9 and HSPD-10. The National Bio and Agrodefense Facility will ensure healthy livestock for the 21st century and protect the public.

- **Low Volatility Agent Warning System .....$20 million**
  An additional $20 million is provided to develop the Low Volatility Agent (LVA) Warning System, which will serve as the basis for a warning and identification capability against a set of chemical threat agents whose vapor pressure is sufficiently low that detection by conventional approaches is exceptionally difficult. This set of low volatility agents includes some of the most toxic materials currently known. The Chemical Countermeasures portfolio has initiated an effort to develop a transportable capability for the detection of these materials in a response and recovery mode. This R&D effort is referred to as LVA Surface Contamination Monitor. The additional FY 2006 funding will be used to develop a protection-mode capability to detect these materials upon release in specific environments. This detect-to-warn system will alert the response system of the imminent hazard and enable protection of potential victims from exposure and permit application of prompt medical countermeasures to minimize or eliminate casualties. This system will be a network of detectors to provide a protect-to-warn capability for specific venues, such as high-value buildings and transit systems. The LVA Warning System will both detect and identify the agent to ensure correct medical countermeasures are engaged.

- **Radiological/Nuclear Countermeasures Test and Evaluation Complex…$9 million**
  The Radiological/Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC), part of the DNDO, will provide the nation with the necessary facilities and capabilities to validate the performance of systems under development, and already deployed, to protect the United States from the threat of a terrorist radiological or nuclear attack. Located on the Nevada Test Site, the Rad/NucCTEC will be a unique national asset, permitting classified high-fidelity testing of radiological/nuclear sensors and sensor systems utilizing strategic quantities of special nuclear materials in realistic configurations.

The Rad/NucCTEC will provide the nation with the capacity to rapidly evaluate the performance of our current and developing homeland defenses against validated threats, using actual radiological and nuclear materials, for which no facility currently exists.

- **Counter-MAN Portable Air Defense Systems (C-MANPADS).....$49 million**
  C-MANPADS' increase of $49 million plus $61 million of base funding equal to a total funding level of $110 million in FY 2006. If deemed appropriate based on the Phase II results and approval from Congress, the Counter-MANPADS Program will initiate Phase III to include delivery and installation of pre-production Counter-MANPADS equipment on commercially operated aircraft by U.S. cargo carriers similar to those aircraft dedicated to meet the Civil Reserve Air Fleet (CRAF) requirement. To foster competition, the additional funds will be used to maintain two contractors in Phase III. In FY 2006, each contractor will update its designs to incorporate new design requirements including reliability improvements, technology protection, and emergency ground notification. Operational testing and evaluation will be performed on multiple aircraft types to capture true operational and maintenance costs as well as technical performance and reliability data. In FY 2006, twenty operational aircraft will be modified and sixteen Counter-MANPADS systems will be procured to support reliability and test data collection and critical technology protection measures. This information is critical to further maturing the life cycle cost impact analysis to the airlines, and the extensive reliability analysis will be used to validate and improve system reliability. Dialogue with Original Equipment Manufacturers (OEM), such as Boeing and Airbus, will be initiated and studies conducted to scope the effort required to include provisions for Counter-MANPADS systems on future production aircraft. Additionally, live fire test evaluations will provide insight into the overall effectiveness of the system installed on commercial aircraft. Finally, Federal Aviation Administration (FAA) certification will be completed for additional relevant aircraft types/models/series not addressed in Phase II.

- **Research and Development Consolidation……....$127.5 million (67 FTE)**
  The Transportation Security Administration (TSA), the United States Coast Guard (USCG), the Bureau of Customs and Border Protection (CBP) and the Information Analysis and Infrastructure Protection (IAIP) will integrate their RDT&E activities with those conducted within the Department of Homeland Security's S&T Directorate. This consolidation will bring the scientific and engineering personnel and other RDT&E resources of the Department under a single accountable authority. The S&T Directorate's vision for this RDT&E integration will be to start the development and expansion of collaborative relationships, foster and leverage an environment of collective capabilities, maximize the efficiency and effectiveness of the Department's RDT&E capacity as well as develop and expand synergistic RDT&E programs that cut across the Department's activities. Bringing RDT&E under the S&T Directorate will allow the other organizational elements to collaborate in the RDT&E integration and to focus on their operational missions, and eliminate within them the specialized management infrastructure required to manage RDT&E. The FY 2006 R&D Consolidation budget is $127,497,000 of which $10,600,000 is in support of 67 FTEs and $116,897,000 is for RDT&E.

In addition to the RDT&E activities conducted at the portfolio level, the Science and Technology Directorate is committed to additional activities that both facilitate and enhance the research

efforts of the portfolios. The Directorate places significant emphasis on its interfaces with other government agencies as well as the transfer of technology to other directorates and agencies.

Studies and Analysis

The Homeland Security Science and Technology Advisory Committee (HSSTAC) and the Homeland Security Institute (HSI) constitute the major activities of Studies & Analysis. Both were established under the Homeland Security Act of 2002 to provide independent scientific & technical analytic expertise to the Department through the Under Secretary for Science and Technology. HSSTAC operates under the Federal Advisory Committee Act. HSI operates in accordance with regulations governing Federally Funded Research and Development Centers. By charter, each engages in substantial contact with other agencies, private sectors, and other entities to facilitate communication, identify issues, and bring the best advice to the Department and the Government.

The Homeland Security Science and Technology Advisory Committee (HSSTAC)

The HSSTAC, established in November 2003, was chartered to be a source of independent scientific and technical planning advice for the Under Secretary for Science and Technology. It is solely advisory in nature and focuses on the responsibilities of the Under Secretary for Science and Technology to organize the Nation's scientific and technological resources to prevent or mitigate the effects of catastrophic terrorism against the United States; identify research areas of potential importance to the security of the Nation; assist in establishing mission goals for the future; advise on whether the policies, actions, management processes, and organization constructs of the Science and Technology Directorate are focused on mission objectives; advise on whether the research, development, test, evaluation, and systems engineering activities are properly resourced (capital, financial, and human) to accomplish the objectives; identify outreach activities; and, review the technical quality and relevance of the Directorate's programs.

During the past year HSSTAC met, either in part or in whole, with the following:

- Port Authority of New York & New Jersey - To evaluate the needs and operational requirements of the BioWatch and Rad/Nuc detection programs.
    - Port Authority Police Department
    - George Washington Bridge
    - Holland Tunnel
    - Howland Hook Marine Terminal
- NYC Office of Emergency Management – To meet with senior leaders and gauge their assessment of the BioWatch program
- NYC Public Health Laboratory - To observe the sample testing phase of the BioWatch program.
- Department of Energy National Laboratories (Sandia National Laboratory, Lawrence Livermore National Laboratory, Pacific Northwest National Laboratory, Los Alamos National Laboratory) - To learn about the various homeland security technology capabilities found in the National Labs and discuss with senior leaders how such laboratories can best serve the nation.

- Food & Drug Administration - The Acting Commissioner and other senior leaders to assess how DHS and FDA determine and implement respective roles and responsibilities regarding disease detection.
- Department of Health and Human Services - Assistant Secretary and senior staff from the Centers for Disease Control to discuss how DHS and HHS determine and implement respective roles and responsibilities regarding disease detection.

Annual Report to Congress: The Committee's overarching conclusions are:

- The S&T Directorate has made notable progress in organizing, establishing processes, establishing relationships with other Department of Homeland Security (DHS) activities and with the broader community relevant to homeland security.
- The Directorate's strategic planning process is underway but needs staffing, clear intent and guidance, metrics useful to set priorities, and methodologies for planning and assessments.
- The Directorate has become the default operator of some fielded systems; focusing on operating fielded systems will divert both attention and resources needed to develop the needed new and improved capabilities.
- The Directorate needs to focus on the needs of multiple publics with distinctly different needs.
- A major objective of homeland security activities should be to build public resiliency to a wide range of possible attacks.
- Understanding a wide range of specific threats is essential to understanding and addressing vulnerabilities to potential disruptive assaults.
- To achieve the national goals in homeland security, DHS needs to take the lead in fashioning a mechanism for coordination and cooperation among the relevant Federal research and development (R&D) activities.
- A larger growth rate is needed to build programs, infrastructure and capabilities.
- The S&T Directorate needs to define in some detail what kind of relationship it believes is needed with the DOE labs to meet DHS needs.

Homeland Security Institute

The Homeland Security Institute is a Federally Funded Research and Development Center (FFRDC) operated and managed by Analytic Services Inc. to provide independent, objective studies and analyses to address critical homeland security issues, particularly those that require scientific, technical, business systems, and analytical expertise. The HSI is a strategic resource for the Department with the Under Secretary for Science and Technology (S&T) serving as primary sponsor on behalf of the Secretary. HSI programs crosscut DHS organizational lines and involve Coast Guard, BTS, EP&R, IAIP, as well as S&T Directorate components. In order to provide dedicated, multi-disciplinary, critical analysis and decision support capability for DHS

department-wide, HSI engages other agencies and broader communities as necessary to better inform DHS and to apply "dual-benefit" approaches directly into program planning.

During the past year HSI conducted the following studies that involved other Federal agencies:

- National laboratory capabilities assessment - conducted an extensive survey of homeland security capabilities resident in the Department of Energy national laboratories
- Cargo summit - facilitated private sector communications and provided analysis on the national cargo security strategy including Department of Transportation, Federal Highway Administration, Department of State, Department of Defense
- Critical Infrastructure Protection Vulnerability Studies with Department of Energy (to include the National Laboratories), United States Department of Agriculture, Food and Drug Administration, Department of Transportation, United States Coast Guard, National Transportation Safety Board, White House Office of Science and Technology Policy, Amtrak
- Wide Area Biological Restoration study involves Environmental Protection Agency, Health and Human Services, National Institute of Health, Department of Defense (U.S. Army Center for Health Promotion and Preventive Medicine), United States Postal Service, Department of State, Department of Energy National Laboratories, Department of Justice, Federal Bureau of Investigation, Central Intelligence Agency, United States Department of Agriculture, General Services Administration, Technology Surprise Working Group, Department of Labor
- Reasons for Successful and Unsuccessful Terrorist Incidents Against the US – Federal Bureau of Investigation, Department of Justice, Department of State
- Threat and Technology Assessments – Central Intelligence Agency, Defense Intelligence Agency, U.S. Army, U.S. Air Force, U.S. Navy, U.S. Marine Corps, National Aeronautics Space Agency, Technology Surprise Working Group, National Ground Intelligence Center, Office of Science and Technology Policy

Division of Effort Among the DHS S&T Directorate and Research Efforts at Other Government Agencies

One of the accomplishments of which I am personally most proud is the emphasis our new Directorate has put on interacting with other Federal departments and agencies. Knowledge of other science and technology programs and their results, appropriate collaboration between agencies, coordination of relevant programmatic activities, and information sharing are essential for us to best meet our mission requirements.

The Science and Technology Directorate recognizes that many organizations are contributing to the science and technology base needed to enhance the nation's capabilities to thwart terrorist acts and to fully support the conventional missions of the operational components of the Department. Congress recognized the importance of the research and development being conducted by numerous Federal departments and agencies, and, in the Homeland Security Act of 2002, directed the Under Secretary for Science and Technology to coordinate the Federal government's civilian efforts to identify and develop countermeasures to current and emerging threats.

We take this responsibility very seriously.

Over the last year, the Science and Technology Directorate has worked with the Office of Science and Technology Policy, the Homeland Security Council, the National Security Council, the Office of Management and Budget and the Office of the Vice President to initiate the effort to coordinate homeland security research and development across the entire United States Government. It will come as no surprise to the members of this Subcommittee that good, solid, effective research and development relevant to homeland security is being conducted by the Departments of Agriculture, Commerce, Defense, Energy, Justice, Health and Human Services, State, and Veteran's Affairs; within the National Science Foundation, the Environmental Protection Agency and other Federal agencies; and by members of the Intelligence Community.

Several interagency working groups already exist that are addressing issues important to homeland security. The Science and Technology Directorate has been, and continues to be, an active participant in these working groups, and in most cases has taken a leadership role. These fora foster an active exchange of information and assist each participating agency in identifying related needs and requirements, conducting research and development of mutual benefit, and avoiding duplication of effort.

We also continue to have discussions at multiple levels of management with Federal Departments and Agencies, as well as with the Office of Management and Budget, the Office of Science and Technology Policy, and the Homeland Security Council. These discussions ensure that the strongest possible links are made and the best possible coordination occurs between our Department and those who are conducting sector-specific research.

A full list of S&T Directorate interagency interactions and their results are listed in the Appendix.

Technology Transfer

We are often asked about the transfer of technologies between Departments. I want to assure you that the Science and Technology Directorate is very concerned about technology transfer. Often, technology developed for one purpose, such as a military application, cannot be transferred in a straightforward manner to civil operations. The requirements for maintenance and support, for performance, and for total cost of ownership often inhibit such transfers. Although the basic scientific principles that underpin a particular technology may be leveraged, nevertheless significant re-engineering is required to make the technology suitable for homeland security purposes.

Other issues associated with transferring technologies to the homeland security operating environment include the need for ease of operations, extremely low total cost of ownership, providing liability relief, providing incentives for non-federal actors to purchase useful technologies, developing and promulgating standards and providing technical assistance to aid those purchasers in their procurement decisions. While the Department has made tremendous progress in all these areas, much remains to be done, and sustained effort is needed.

Short-Term and Long-Term Research

In the two years that this Department has been in existence, the Science and Technology Directorate has focused its efforts on near-term development and deployment of technologies to improve our nation's ability to detect and respond to potential terrorist acts. However, we recognize that a sustained effort to continually add to our knowledge base and our resource base is necessary for future developments. Thus, we have invested a portion of our resources, including our university programs, toward these objectives. The following table indicates our expenditures in basic research, applied research, and development to date.

Science and Technology Directorate R&D Investments (in millions of $)			
Fiscal Year	**FY 2004(actual)**	**FY 2005(estimated)**	**FY 2006(proposed)**
Basic	68	85	112
Applied	243	340	399
Developmental	470	587	746
Total	**781**	**1012**	**1257**
% Basic	**8.7%**	**8.4%**	**8.9%**

Our expenditures in basic research are heavily weighted by our investments in university programs. These university programs will not only provide new information relevant to homeland security, but will also provide a workforce of people who are cognizant of the needs of homeland security, especially in areas of risk analysis, animal-related agro-terrorism, bioforensics, cybersecurity, disaster modeling, and psychological and behavioral analysis.

Basis for Policy on the Use of the National Laboratories

The Department of Homeland Security recognizes the unique technical expertise and infrastructure at the Department of Energy national laboratories. The Science and Technology Directorate has and will continue to maximize and leverage the existing capability base at the national laboratories to address DHS strategic objectives. The S&T Directorate will use strategic partner laboratories to assist in developing program direction, and we will make strategic investments in the national laboratories to build an enduring national capability for DHS. For example, the S&T Directorate is creating technical centers within the national laboratories where expertise currently exists in specialized areas, such as a visual analytics center and a biodefense knowledge center.

The Directorate submitted a Report to Congress on the "Utilization of the National Laboratories" last October which describes the Science and Technology Directorate's policy regarding the use

of the national laboratory resources. The report details how the Science and Technology Directorate has translated its performance-based management philosophy into annual rigorous processes for program planning, program execution, and program reviews. Through this annual cycle, work performed at each of the laboratories is peer reviewed and funding decisions for the following year are based on the annual performance reviews.

Staffing

When the Department of Homeland Security stood up on March 1, 2003, the S&T Directorate had a total staff of about 87, including the 53 staff transferred from the Department of Energy's Environmental Measurements Laboratory.

Two years later, we have a staff of nearly 450, including 167 DHS employees, Nine Public Health Service Officers, 32 Intergovernmental Personnel Act employees, 17 individuals on assignment from other agencies, and 223 contractors.

We continue to be active in staffing our Directorate with well-qualified individuals whose skills support the full breadth of our responsibilities and RDT&E activities. We continue to actively seek additional staff in accordance with our approved staffing plan.

Conclusion

With nearly two years under the Department's belt, the scientists and engineers in the Science and Technology Directorate have accomplished more than I could have expected. I am proud to have shared with you today some of those success stories. We have appended a more comprehensive summary of accomplishments to date for the record.

We also recognize that there is much to do, and we will be working just as hard in FY 2006.

I look forward to continuing to work with the Science Committee, my colleagues here today, other Federal departments and agencies; the academic community; and private industry to continue the work begun and continually improve our ability to protect our homeland and way of life.

Appendix A

Accomplishments of the Science and Technology Directorate

Department of Homeland Security

FY 2004 to February 2005

Biological Countermeasures

- Deployed additional environmental sensor systems to new metropolitan areas to protect our nation's cities from the threat and ramifications of a bioterrorist attack. BioWatch activities were significantly increased during the National Code Orange Alert (December 2003-January 2004), with twice daily samplings in the high threat cities, additional collectors for special New Year's events and Bowl Games, and deployment of temporary BioWatch systems to non-BioWatch cities of special concern. BioWatch also provided field and laboratory support to the G8 Conference, the Democratic National Convention, and the Republican National Convention in Boston and New York, respectively.

- Continued to develop new technologies to support biosurveillance and detection. Two detection R&D programs transferred to DHS from the DOE's Chemical and Biological National Security Program (CBNP) are reaching their successful conclusion. The Autonomous Pathogen Detection System that provides for totally automated integrated sample collection and analysis is now undergoing field-testing in New York City, while the hand-portable chemical and biological detection system known as micro-ChemLab is one of the leading contenders for the next generation DoD Joint ChemBio Modular Detector. High throughput processing techniques that will greatly increase BioWatch capability have been developed and are being piloted as part of the second generation BioWatch system known as Gen 2 BioWatch. This pilot is in the process of being deployed in New York City and will involve a two-to-threefold expansion of the number of collectors at locations to be specified by the city (e.g., high profiles venues, subways, transportation hubs) with an even greater increase in sample analysis capability so as to support surge activities and the extensive follow-on analysis that would have to be done in the wake of an actual event. Efforts are underway in the BioNet program to develop integrated concept of operations with civilian and military bio-monitoring systems (e.g., BioWatch and the Joint Service Installation Pilot Program (JSIPP)/Guardian) using San Diego, California, as the pilot site. Solicitations and awards for next generation biological detection systems to support a fully automated BioWatch (Gen 3) and to enable very rapid detection (about 2 minutes) for protecting special events and selected facilities have been made. However, these detection systems are only as good as the underlying bioassays which recognize the agents of interest. These assays are designed to detect multiple features in an organism so as to produce very low false alarm rates, less than one in a million.

- Initiated the design of National BioSurveillance Integration System (NBIS) as part of an interagency process. When completed in the first quarter of FY 2005, we will work with the Information Analysis and Infrastructure Protection (IAIP) Directorate to implement this system.

- Developed a set of ChemBio Defense Guidelines for Airports that are currently out for review at five major airports around the country through the Protective and Response Options for Airport Counter Terrorism (ProACT). This program, The Airport Restoration Demonstration, at the San Francisco International Airport (SFO), is working with EPA, CDC and SFO to develop a set of pre-approved protocols and decontamination agents for decontamination and return to service of major airport facilities. As part of this, the National Academy of Sciences is conducting a study of "How clean is clean?" the final report will be completed in the spring 2005. Work is on-going on improvements to technologies for facility clean-up, including improvements in chlorine dioxide and vaporous hydrogen peroxide approaches and the completion and testing of a truck-deployed chlorine dioxide based decontamination system.

- Using the reference scenario approach recommended by HSPD-10 for understanding the requirements of an integrated national biodefense architecture, the portfolio will complete the high-level analyses of four baseline references cases: a large outdoor release of a non-contagious agent (anthrax); a large indoor release of a contagious agent (smallpox); contamination of a bulk food supply; and two highly virulent agricultural attacks, one on livestock (Foot and Mouth Disease) and the other on plants (soy bean rust). Completion of the architectures will identify key requirements for each major element, a "report card" on the current and projected status in that area and performing detailed design tradeoffs for those areas in which DHS has execution responsibility

- Two material threat determinations have been made (anthrax and botulinum) in support of BioShield and risk assessments have been performed to help understand the plausible worse case scenarios and help guide the size of the BioShield procurements.

- BASIS was used to provide additional support for the designated National Special Security Events (NSSEs) to include the 2004 G-8 Conference, and the Democratic and Republican National Conventions.

- A National Strain Repository will be established to allow comparison of suspect samples with known existing strains. Genotyping assays will be completed for anthrax and be well underway for the next two high priority agents determined by NBFAC and the law enforcement community.

- Initiating operations in interim facilities until completion of construction of the new NBACC facility currently scheduled for FY 2008/2009. Arrangements have been made for use of BSL-2/3 aerosol laboratory capabilities through partnerships and agreements with Lovelace Respiratory Research Institute, Battelle Memorial Institute and the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and for use of BSL-2/3/4 with DoD, USDA Food Safety and Inspection Service (FSIS), and CDC.

- A systematic biothreat risk analysis process has been initiated with broad involvement from government, industry and universities. Technical support has also been provided to the Emergency Preparedness and Response Directorate of DHS and to the CDC to assist in understanding the requirements on the Strategic National Stockpile.

- HSPD-10 designates the National Bioforensics Analysis Center (NBFAC) as the lead national facility for technical analysis of forensic samples from biological events. Pending completion of the NBACC construction, a 3,000 square foot dedicated microbial forensics laboratory has been established at USAMRIID and is currently handling some 1500 samples. A joint governance model is being developed with the FBI and others and a broad based interagency meeting was held to identify R&D requirements.

- Successfully addressing operational issues at the Plum Island Animal Disease Center (PIADC). Improved security procedures have been implemented and a new Operations and Maintenance Contractor is in place. An integrated USDA-DHS research strategy, and development, including a detailed veterinary countermeasures and diagnostics strategy, has been developed. R&D programs have been initiated to evaluate improved variants of commercial animal vaccines, develop and deploy the next generation multiplexed diagnostics assays to rapidly and unequivocally identify foreign animal diseases (FAD) such as Foot and Mouth Disease (FMD), and to implement a bioforensics capability for FADs.

Chemical Countermeasures

- Initiated a process to define the requirements and process for a robust national environmental analytical laboratory capability through a core interagency working group including EPA, CDC, and other stakeholders under DHS Chemical Countermeasures leadership. The design of triage laboratory capability to support analyses of complete unknowns was completed. The portfolio conducted preliminary activities toward the development of a Chemical Security Analysis Center (CSAC) that will provide threat awareness and assessment. An overall structure, similar to that characterizing the NBACC and its supporting threat characterization, forensics, knowledge management and reachback, is envisioned. Interfaces with the FBI and Scientific Working Group for Forensic Analysis of Chemical Terrorism (SWGFACT) identified shortfalls in current forensics capabilities and infrastructures and facilitated the initiation of a comprehensive program to address technical deficiencies. Baseline forensics signatures were established, and an initial set of laboratory forensics protocols were developed.

- Initiated prototype development for a Mobile, High-Throughput Lab ID System. This system is a self-contained mobile laboratory for on-site chemical analysis of a high volume of samples to support comprehensive assessment of a chemical incident scene and to monitor progress of restoration activities. There is no current capability for on-scene assessment and screening of environmental samples to streamline the process of remediating a contaminated site. As has been demonstrated by previous cases of chemical contamination of the environment, very large numbers of samples must be analyzed to determine extent of contamination and then support decisions to re-use after decontamination procedures. Accordingly a high-throughput (possibly 1000 per day)

sample stream must be supported. Design the concept and demonstrate the prototype in 2005. .

- Development of a playbook containing restoration protocols following a chemical incident was initiated. Studies were initiated to develop and evaluate decontamination technologies for non-traditional agents.

- Deployed a chemical threat detection system to Boston and New York City transit stations for the Democratic and Republican National Conventions, respectively. The system will also be deployed for the 2005 Presidential Inauguration. The system was based on the Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) chemical agent detection system recently transitioned to the Washington, D.C., Washington Metropolitan Area Transit Authority (WMATA) metro system, which has operated for a year without a false alarm. The system provides prompt detection of a chemical attack to effect optimal response actions. The system deployed to New York City is being left in place as an initial permanent capability.

- Initiated systems studies around three defining scenarios: indoor chemical agent release, outdoor toxic industrial chemical release, and release of toxin in the water system. Primary components of these defining architectures were developed and serve as the basis for continued definition of capability gaps and required improved countermeasures. Development of these architectures and resultant guiding principles will be coordinated with DHS IAIP as well as other government agencies to maximize cross-agency leverage. Three demonstration projects were also initiated: The Facility Restoration Demonstration Project will develop and demonstrate a capability to restore a facility that has been contaminated with a classical chemical agent or persistent toxic industrial chemical (TIC). A Water Security Demonstration will identify and characterize technologies with the potential to provide warning of chemical contamination of the water system. A NSSE Deployable Detection System Demonstration will develop a flexible architecture chemical detection system that can be utilized for the warning and situational awareness of chemical threats in temporary deployments.

- Initiated key development programs targeting leap-ahead advancements in detection. These programs will develop two principal capabilities: a facility monitoring detector and a responder detection tool. In both cases, the detectors will provide detection and discrimination of up to 20 different chemical threats, including classical chemical warfare agents (CWAs) and toxic industrial chemicals (TICs) in a single unit across a wide range of concentrations. Current chemical detectors address far fewer chemical agents. These new detectors will be network-compatible to provide comprehensive situational awareness and, in facilities, will initiate response actions to mitigate the threat as appropriate. A workshop was conducted to gather and discuss technology solutions for the challenge of detecting very low vapor pressure chemical hazards. A program to develop such technologies was formulated.

Radiological and Nuclear Countermeasures

- Presently developing new capabilities and a corresponding architecture for detection of nuclear materials through a new coordinating office, which will outline an investment strategy for nuclear material detection R&D as well as procurement and deployment of next-generation technologies.

- Expanded secondary-reachback to include all instrumented Customs and Border Protection's POEs and personnel, and U.S. Coast Guard special teams: Expert reachback required to resolve highly suspicious or highly anomalous alarms will be expanded to cover all sites and personnel within the Bureau of Customs and Border Protection (CBP) and USCG that use/carry radiation detection equipment.

- Radiological and Nuclear Countermeasures Test and Evaluation Complex: Provides capability to conduct controlled field testing of special nuclear material (SNM) in their most relevant configuration in mock essential operational venues. Initial capabilities will come on-line at the end of 2005.

- Assumed management of the Port Authority of New York and New Jersey radiation detection test bed from the Department of Energy in August, 2003. Following the transfer, the portfolio broadened the project scope beyond testing and evaluating individual pieces of technology to a systems approach, including response protocols and operational concepts. This program has been renamed the Countermeasures Test Bed to more accurately reflect the span of the project.

- The portfolio will initiate a joint DHS/HSARPA and DoD/DARPA (Department of Defense/Defense Advanced Research Projects Agency) project focusing on radiological and nuclear decontamination, consisting of four main tasks: (1) Radionuclide capture decontamination; (2) Wide area radionuclide decontamination; (3) Verification; and (4) Modeling.

- Further efforts will begin under the Environmental Measurements Lab's (EML) Urban Dispersion Program (UDP), an atmospheric dispersion modeling effort to model the release of airborne hazardous materials in New York City. Initial work on this project will begin with radiological and meteorological network installation plans as well as survey measurements of SF_6 (tracer) background in the city being completed this year. Additionally, a crisis response scenario analysis was conducted to identify technologies and capabilities needed for crisis response. EML is also currently running the Incident Management Radiological Monitoring Network in New York City, an operational test bed for radiation sensor systems that can be used for search and characterization by local first responders. In August 2004, additional sensor nodes were installed and established throughout the city, at sites selected in conjunction with New York's Office of Emergency Management (NYCOEM).

- Needs and technical approach analyses for both passive and active interrogation detection technologies. Several advanced passive detector technologies are in the early stages of development: an inexpensive, deployable, high efficiency neutron sensor; a large area

combined neutron/gamma detector; a large-volume high-pressure xenon (HPXe) detector; a directional detector for fast neutrons; and a mercuric iodide (HgI_2) detector. The large-volume HPXe detector is currently in the prototype phase. Also in development are two gamma-ray imaging systems, one based on Compton imaging and the other on coded aperture imaging; both are currently in early prototyping phases. Additional efforts focused on the detection of shielded SNM in cargo containers, based on the detection of both neutrons and delayed high-energy fission product gamma rays, and a portable neutron source, based on a mixed alpha-Be source in a switchable configuration for use in active interrogation; both currently are still in conceptual design and experiment phases.

- Improvements in two current Customs and Border Protection-deployed radiographic imaging systems. This included software improvements and systems upgrades for local data integration, threat image projection (TIP), and assisted imaging processing (AIP). Efforts are expected to begin in the 4th Quarter of FY 2004 for work on near-term improvements in hand-held radioisotope identification (RIID), area search devices with radioisotope identification, passive primary portals, advanced radiography systems for cargo and parcels, and advanced active imaging and screening systems.

- An additional effort is directed towards a comprehensive chemical, biological, radiological and nuclear (CBRN) water system vulnerability study.

- Further efforts were begun under the Environmental Measurements Lab's (EML) Urban Dispersion Program (UDP), an atmospheric dispersion modeling effort to model the release of airborne hazardous materials in New York City. Initial work on this project has begun, with radiological and meteorological network installation plans as well as survey measurements of SF_6 (tracer) background in the city being completed this year. Additionally, a crisis response scenario analysis was conducted to identify technologies and capabilities needed for crisis response. EML is also currently running the Incident Management Radiological Monitoring Network in New York City, an operational test bed for radiation sensor systems that can be used for search and characterization by local first responders. By August 2004, additional sensor nodes will have been installed and established throughout the city, at sites selected in conjunction with New York's Office of Emergency Management (NYCOEM).

Explosives Countermeasures

- Initiated the development of a prototype explosive detector for vehicle bombs, and accelerated the development of hardened overhead storage bins for passenger aircraft. Additionally, it initiated a survey and evaluation of commercial-off-the-shelf (COTS) equipment to detect, interdict and mitigate the consequences of suicide bombers and vehicle bombs, and conducted a cost-benefit analysis of approaches to aircraft hardening.

Threat and Vulnerability Testing and Assessment

- Delivered two operational components, the Threat Vulnerability Integration System (TVIS) and the Threat-Vulnerability Mapper (TVM), to the IAIP Directorate. The TVM provides counterterrorism analysts with a simple, straightforward way to depict the

geographic distribution of threats across the U.S. and to search the underlying databases for information on the possible actors, agents, potential severity of attacks, and extent of the vulnerabilities to and effects of such attacks. TVIS integrates high-volume information analysis capabilities with specialized visualization tools that enable analysts to process large amounts of disparate intelligence data.

- Created the Interagency Center for Applied Homeland Security Technology (ICAHST) capable of addressing the technical needs of the Department and other members of the Homeland Security community. The center and its interconnected laboratories provides detailed technical information and guides research, strategy, and systems design for the broad range of technologies and techniques necessary to identify, understand, and remediate CBRNE threats. The center consolidates and validates the S&T Directorate's and other customers' technical requirements as well as performs comprehensive technical evaluations of technologies either available through commercial, academic, or government sectors or being specifically developed through the various TVTA research programs. The ICAHST activity is supported by an interagency Steering Group with representatives from 23 intelligence and law enforcement agencies.

- Completed an initial set of 120 all- CBRNE capability assessments for 20 terrorist organizations on the five CBRNE plus cyber threat agents. Continued support to the Nuclear Assessment Program (NAP) that judges the credibility of communicated nuclear threats for such clients as the FBI, DOE, and Department of State (DOS).

- Created the National Visualization and Analytics Center (NVAC). NVAC creates a national agenda document for visual analytics with broad input and support from the government, national laboratories and universities and provides the following four core functions: research and development, education, technology evaluation and implementation, integration and coordination. NVAC is expected to address the intrinsic challenges of:
    - Dealing with massive streams of information in support of the analysts;
    - Visualization of information for detecting deception and resolving uncertainty;
    - Visualization of temporal primary and supportive theme relationships critical for proactive and predictive analytics; and
    - New, multi-dimensional visualization tools for human-information discourse, which enable analysts to query, cluster or group, and manage multiple types (for example, databases or unstructured text) and modes (such as text, audio, video, imagery, or sensor) of data or information as well as incomplete data streams.

- Establish an integrated, national capability, called the Institute for Discrete Sciences (IDS), to investigate and develop the specialized computing algorithms and hardware architectures necessary to analyze massive amounts of diverse data from multiple, disparate, distributed data sources, and to model terrorist attacks and simulate consequences on a real-time, high-resolution basis. Like the NVAC, the IDS will have broad interaction and support from the government, national laboratories and universities.

- Complete an engineering design for the Enhanced International Travel Security (EITS) system, initiated in FY 2004, which will enable several pilots to be implemented with the United Kingdom, Canada, and Australia. EITS allows the validity of travel documents and the identity of travelers to be determined in real-time at U.S. borders and other points of entry.

- Provide the science and technology needed in the development of biometrics for precise identification of individuals, and develop prototype instrumentation to aid authorized officials in detecting individuals with potentially hostile intent.

- Enable a comprehensive capability for determining terrorist motivations, based on social, behavioral, and economic factors. Integrate this with techniques for determining terrorist or hostile intent as well as detecting deception.

Standards

- Continued development of the First Responder Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) Protective and Operational Equipment Standards Development Program, an ongoing comprehensive, multi-year program that is developing an integrated suite of national standards for emergency responder CBRNE protective and operational equipment.
- Developed standards that address radiation protection for all activities corresponding to the EP&R mission.
- Developed comprehensive standards for the development, testing, and certification of effective detection, response, remediation, and forensics tools for radiological and nuclear materials.
- Composed three management directives to establish DHS policy with regards to the adoption and development of national standards. Two of the management directives dealing with DHS internal standards policies have been issued. In addition to establishing policy, the standards program has engaged with the American National Standards Institute (ANSI) to develop a searchable database containing existing standards related to homeland security and to establish the ANSI Homeland Security Standards Panel.
- Formed an interagency task force to address the controversy over the effectiveness and use of lateral flow immunoassays for the detection of *Bacillus anthracis* (anthrax) by emergency responders. Five commercially available hand-held immunoassays and two reference methods have been tested and evaluated in a multiple laboratory study. Other accomplishments in biological countermeasures include an effort with Edgewood Chemical Biological Center (ECBC) to evaluate a five step method to pre-screen suspicious white powders, an effort with NIST to look at the effectiveness of biological agent simulants, and the establishment of a program to address both chemical and biological decontamination standards for the first responder community. A draft standard for a hand-held vaporous chemical warfare agent detector was developed. A project was initiated to provide both physical standards and validated spectral libraries necessary to impart confidence in the performance of portable Raman spectrophotometers (currently

in use by first responders to identify unknown substances in real-time with minimal handling). Other accomplishments include participation in the development of Protective Action Guides following a RDD/IND event; the development and adoption of the first radiological and nuclear detector for four classes of radiation detection equipment ranging from hand-held alarming detectors to radiation portal monitors for cargo containers; the development and evaluation of the four accompanying test and evaluation protocols; testing of relevant COTS radiation detection equipment; production of standardized test sources (γ-ray, neutron); and the initiation of an effort to develop performance specifications for active interrogation systems (x-ray, gamma-ray, and neutron imaging) used in the detection of SNMs. High explosive countermeasures initiatives include standards for explosives reference materials, trace explosive detection devices, and explosive mitigation equipment standards. The high explosives standards program is leveraging programs funded by the Department of Justice's National Institute of Justice to develop performance metrics for bomb disposal robots, and to develop a bomb suit standard. Cyber Security programs were initiated to address E-Authentication (for remote authentication techniques), Forensics for Personal Digital Assistant (PDA)/Handheld Devices, and Checklists for Securing Operating Systems and Application Configurations. Specific accomplishments include an exploratory workshop on knowledge based authentication, general approach to password authentication strength, guidance document on PDA forensic policies, guidance document on current forensic software for PDAs, draft guideline for the overall Security Configuration Checklists Program, and a draft Special Publication 800-68 Guide for Securing Microsoft Windows XP Systems for IT Professionals. A list of prioritized requirements for CBRNE countermeasures standards will be constructed based upon the interagency working group's efforts. In addition, a report and database on existing CBRNE countermeasures standards will be issued. New standard development will focus on validation of existing, high priority, high use technology for CBRNE detection Polymeric Chain Reaction (PCR) devices, Raman spectrophotometers, spectroscopy based portal monitors, neutron detectors, high energy x-ray interrogation systems, neutron interrogation systems, trace explosive detection devices, and explosion mitigation devices). In addition, work on characterizing the performance of candidate CBRNE simulant and reference materials will expand. Efforts will be expanded in the area of CBRNE decontamination standards. Efforts will be initiated to develop COTS and Government-off-the-shelf (GOTS) CBRNE equipment consumer report guides based on FY 2004 testing results. To address Cyber security standards the programs for E-Authentication, Forensics for PDA/Handheld Devices and Checklists for Securing Operating Systems and Application Configurations will be continued, along with a new start to develop a Standardized Mechanism for Universal Access Control to enable and promote sharing of information across organizational boundaries each with potentially different access control policies. The standard access control mechanism program will survey existing access control policies and models identify and document access controls most primitive and atomic principles and functions and design a universal access control mechanism capable of abstracting, combining and enforcing all existing attribute based access control policies.

- A standard for full frontal facial photographs entitled "Face Recognition Format for Data Interchange" developed by the International Committee for Information Technology

Standards (INCITS) is currently in the process of being formally adopted by DHS. A biometrics working group was established to gain consensus on the adoption of the standard. A contract is being negotiated with INCITS that will give access to the standard to DHS employees and contractors via the DHS website. Supported a program to develop a portable, externally deployable, biometric acquisition and information system, designed specifically for collecting data for evaluation.

- Continue work with ASTM International to obtain final approval for the Hospital Preparedness Standards and the METL standard for first responders. New initiatives with ASTM on homeland security standards will include a standard guide for building event dispersion and health assessment preparedness and response planning, a standard guide for conducting emergency preparedness drills and exercises, and a standard guide for developing model emergency operations plans in response to all-hazard events including CBRNE. DHS will support EML to initiate a cooperative interagency effort to address laboratory emergency response measurement protocol development and laboratory capability and capacity assessment. Work with National Incident Management System (NIMS) Integration Center (NIC) and Urban Search and Rescue (USAR) robotics standards will continue.

- Supported efforts with American Society for Testing and Materials (ASTM) to coordinate the development of a draft standard for hospital preparedness and to develop a multi-disciplinary Mission Essential Task List (METL) based on Emergency Responder Guidelines developed by the Office of Domestic Preparedness. Supported the EML along with the Council of Ionizing Radiation Measurements and Standards (CIRMS) to organize several sessions to gather information on standard operating procedures and method standards that would be used in data collection, sample preparation and analysis, data reduction, as well as data reporting. To address requirements outlined in the National Incident Management System (NIMS), S&T Directorate is supporting an effort to catalog existing incident management standards and identify and address gaps. Initiated an effort with the NIST to develop comprehensive standards related to the development, testing, and certification of effective technologies for sensing, mobility, navigation, planning, integration, and operator interaction within urban search and rescue robotic systems.

- Supported the development of a number of respiratory standards including three National Institute for Occupation Safety and Health (NIOSH) standards and one National Fire Protection Association (NFPA) standard adopted by DHS in February 2004. The adopted respiratory protection standards address open-circuit Self-Contained Breathing Apparatus (SCBA), CBRN Full Facepiece Air Purifying Respirator (APR), CBRN Air-Purifying Escape Respirator, CBRN Self-Contained Escape Respirator. To date, 50 separate models from six major manufacturers of SCBA have been certified, and two models of APRs have been certified.

- Established ties with the training community including the Center for Domestic Preparedness and local and state organizations. The S&T Directorate has also reached out to determine the necessary requirements and needs for training standards by

participating and supporting the ANSI's Homeland Security Standards Panel Subcommittee on Training. Currently establishing the process by which training standards requirements will be compiled and prioritized. In addition, the development of standards to address training to current DHS adopted radiation detector standards is in progress.

- Initiated efforts to supplement those supported by the Wireless Public SAFEty Interoperable COMmucations (SAFECOM) program. Initiated an effort with NIST to define wireless communications requirements and approaches for urban environments, to develop emergency response operations equipment standards dealing with tactical information from building sensors and systems, wide-band characterization of the dielectric properties of building materials, the definition of wireless ad hoc and personal area networks public safety requirements, and the development of an overall security model for information sharing. These efforts support the integration of communications equipment with protective equipment used during incident response.

- Established the Geospatial Working Group Subcommittee on Standards (with the support of the DHS Geospatial Management Office) to address the adoption of a suite of Geospatial related standards. Work will continue under the auspices of the Geospatial Working Group Subcommittee on Standards. The group will review the compilation of standards recommended for adoption and achieve consensus on the adoption of all relevant Geospatial standards.
- Supported an effort at NIST to work with the American Society of Mechanical Engineers (ASME) to prepare for acceptance a suite of standards and materials for a training course on how to apply the homeland security standards to aid the owners and managers of constructed facilities in the selection of cost-effective strategies for the management of risks associated with terrorist and natural hazards.

- Established the framework for a DHS conformity assessment working group, consisting of experts from DHS, other Federal agencies, and the private sector. Other accomplishments include a draft certification program for radiation detectors affected by the DHS adopted ANSI N42 Radiation Detection Standards; the development and deployment of a conformity assessment training module; outreach to the private sector through the ANSI's Homeland Security Standards Panel and the American Council of Independent Laboratories; and the identification of viable private sector laboratory, certification and accreditation resources that have the competence and capacity to perform selected functions.

Emergency Preparedness and Response

- The Interagency Modeling and Atmospheric Assessment Center (IMAAC) is a DHS-led capability that provides a single hazards prediction for airborne release of hazardous material. The IMAAC coordinates Federal atmospheric support for "incidents of national significance" and provides hazards predictions to Federal, state and local responders. The IMAAC began operation in FY 2004, supporting the National Exercise Program and special events, such as the Democratic and Republican National Conventions. IMAAC

has established near-real time connectivity to the Department of Homeland Security Operations Center and the FEMA National Emergency Operations Center.

- Selected four urban areas were selected for the pilot Regional Technology Integration (RTI) initiative. These locations provide an opportunity to evaluate geographic and governance diversity as well as variability in threats and vulnerabilities. An integrated assessment process has been initiated in collaboration with these communities. These assessments will identify key assets, review existing vulnerability and threat assessments, emergency preparedness and response plans with the express purpose of identifying potential technology systems that can help prevent, detect, respond to and recover from terrorist and other major emergencies.

- Leveraged the work initiated by ODP and the Memorial Institute for the Prevention of Terrorism, the National Institute of Justice and the Department of Defense in identifying needs and gaps as well as existing technology development programs that can be utilized for incident management training. Developing a rapid prototype of the Technology Clearinghouse "hub and spoke" concept to enable first responders to access important information on existing and emerging technologies, training, and relevant standards through a single knowledge portal.

- Established an R&D program that seeks materials and technologies that can be used in multi-hazard environments, applicable to diverse users, and function as an integral part of a more complex personal protection system. Focus is on materials that are lighter-weight or likely to impact on weight reduction of the overall personal protective system, that are robust and able to withstand the challenges of strenuous activity in unstable and uncertain conditions (rubble, collapsing structures, flying debris, etc.) and environments (extreme heat or cold, wind, rain, flash fire) and provide protection against a multitude of hazards (industrial chemicals, chemical or biological warfare agents, radiation, shrapnel, flying debris, other).

- Unified Incident Command and Decision Support: The research and development program in UICDS seeks to harness innovative ideas in an effort to create an information management and sharing architecture specifically designed to meet the needs of incident commanders and emergency responders throughout the nation. It further seeks to realize a robust, fully functional UICDS information management system to enhance the safety and effectiveness of the nation's emergency responder community. This program will confront the technical challenges associated with the development of innovative, modular, scaleable, and secure information management architecture. Utilizing this systems approach will enable incident commanders to capture important incident-related information, analyze captured information, more effectively disseminate mission critical information to emergency responders, present decision guidance options for incident commanders, more finely coordinate the efforts of emergency responders, and store relevant information for future study.

Border and Transportation Security

- Issued a solicitation for an Advanced Container Security Device to develop and field-test the next generation of shipping container security devices, building on the current efforts through Operation Safe Commerce as well as current BTS policy efforts to develop and implement performance standards for container security. The Advanced Container Security Device Program is part of a "Future Smart Container" initiative encompassing container security, communications, and data systems for the future. The goal is to develop and field-test the next-generation of shipping container security devices that are not currently available in the marketplace.

- Supported BTS in putting technology in the field to support the Arizona Border Control Initiative. The program funded the effort to put Unmanned Aerial Vehicles into operation to support surveillance activities. Demonstrated other technologies such as a long range acoustic device which allows agents to communicate from a safer stand-off distance to determine the intent of people. These opportunities allowed the BTS portfolio to evaluate new technologies that could improve the safety and effectiveness of our border patrol agents.

- Conducted a series of officer and agent workshops to understand the operational environments, functional capabilities needed, and associated goals. In addition, a series of technologist workshops were conducted with Federal, industry and academia experts to examine the technologies needed to fill the gaps in capabilities identified during the operators' workshops. Because not all gaps can or will be solved by technology, those gaps that do not lend themselves to technological solutions were referred to BTS management for their information and attention. Added a Scenario Game feature to some of the workshops. The purpose of these scenario-based seminar games was to highlight and validate areas for investment and high pay-off, focus on national impact of technology decisions, examine requirements across components, and analyze the strengths, weaknesses, opportunities and threats of current procedures and technologies.

- Developed a BTS Technology Vision. Together, the elements of this vision - Border Watch, Transportation Watch and Border Net - will significantly improve our ability to provide the information necessary to secure our borders. The foundation of the vision is an architecture and a set of technology programs that will gather, process and distribute real-time knowledge of the border and transportation situation and provide decision support tools and labor saving devices for our security forces.

U.S. Coast Guard

- Integrated a major developmental program, HAKWEYE, into a USCG operational prototype Sector Command Center in South Florida. The HAWKEYE program demonstrates innovative technologies (such as Maritime, Surveillance, Command & Control, Sensor Fusion, and Communications) allowing simultaneous evaluation of technology performance as a direct impact on mission execution. The Operational Assessment of initial equipment installations of HAWKEYE at Ft. Lauderdale, Miami, and Key West will be conducted this year. Focused on the introduction of automated

scene understanding and sensor/data fusion technology (a requirement for meeting manning constraints.

- Expedited the operational evaluation deployment of a new application for an underwater imaging device that was in a long-term development program within the Office of Naval Research. The device's development as a small boat mounted underwater inspection device for threats such as improvised explosive devices or parasitic contraband attachments on vessels or piers. The device will allow the Coast Guard or other maritime security interests with the ability to rapidly inspect critical vessels or maritime infrastructure.

U.S. Secret Service

- The Emerging Threats Program supports the Secret Service's continuing, comprehensive assessments of emerging threats and evolving technologies that pose a threat to dignitaries and assets protected by USSS personnel. This effort centers on the annual analysis of the common attack methodologies, strategies and models of operation currently being enacted against assets of a similar nature to those protected by the USSS. This analysis is to be based on open text information without any information as to the defense, mitigation, and protection models being enacted by the USSS.
- The Law Enforcement Virtual-Reality Training Model program supports prototyping and deployment of a law enforcement security-oriented simulation training system for the USSS-specific training and modeling. Additionally, this system will enhance the effectiveness of emergency responders during actual events.
- The Critical Structure Protective Initiative (CSPI) program will ensure continued research and development of network protection systems and procedures designed to mitigate exploitation of site-specific "Very Large Scale Integration" (VLSI) control architectures.
- The Wireless Tracking Device program supports development of a handheld, man-portable wireless tracking device for locating operators of wireless communication device(s) in difficult radio frequency environments such as an office building or event stadium.

Emerging Threats

- Established informal partnerships with the intelligence community and with the USSS portfolio to leverage ongoing activities in support of over-the-horizon assessment.

- Initiated efforts Emerging Threats, in combination with the Rapid Prototyping portfolio, in both near-term and breakthrough solutions to homeland security issues.

- Held a privacy protection workshop in which the technical and policy communities interacted to identify important technical challenges and high impact solution areas. Information from this workshop will form the basis of upcoming programs in this area.

- Analyzed multiple radar technologies and other surveillance strategies to determine which combination of technologies would best support coastal surveillance by the USCG.

- Conducted three sensitive projects, two in collaboration with the USSS and one addressing a critical infrastructure.

- Sponsored studies at the Homeland Security Institute to identify threat and technology trends and develop a framework for analyzing emerging and future threats to homeland security.

Rapid Prototyping

- Solicited ideas, concepts and technologies for 50 requirement areas of interest to both the Department and other agencies. Efforts have been initiated to address chemical and biological threats, explosive detection, training technology tools, improvised nuclear device defeat, and investigative and forensic support topics.

- Developed a joint port and coastal surveillance prototype designated HAWKEYE with the United States Coast Guard (USCG) that provides an integrated maritime surveillance system covering Port Everglades, Miami, and Key West, Florida. This first-of-its-kind integrated command center and maritime surveillance facility opened in July 2004.

- Initiated the implementation of the Technology Clearinghouse as required in the Homeland Security Act of 2002. This clearinghouse serves as the central nexus to the public safety and first responder community on: (1) Information services supporting access to, and dissemination of, information regarding innovative technologies serving the DHS mission; (2) Resources designed to support the collaborative needs of teams serving the mission of DHS; and (3) Technology programs and resources themselves, designed to serve the mission of DHS and distributed via a central DHS mechanism. The clearinghouse will integrate these existing databases though a "hub and spoke" configuration and allow a single point of access to multiple disparate information sources.

- Initiated efforts, in combination with the Emerging Threats portfolio, in both near-term and breakthrough solutions to homeland security issues. Near-term projects are funded out of the Rapid Prototyping Portfolio. Breakthrough projects are funded from the Emerging Threats Portfolio.

- Initiated a program to demonstrate an improved fire fighting protective ensemble and continued its further development. These next-generation garments will provide dramatically enhanced protection against chemical and biological agents while improving the flexibility, weight, durability, heat stress reduction, service life, and costs associated with currently available protective gear.

- Development is underway in the Rapid Prototyping portfolio on technologies that will enable response coordinators to locate, track, monitor, and communicate with emergency responders in structures.

Counter-MANPADS

- Initiated and completed Phase I. In January 2004, following a competitive bidding process, DHS awarded Other Transaction (OT) for Prototype Agreements (OTA) to three companies – BAE Systems, Northrop Grumman, and United Airlines – for Phase I of a two-year System Development and Demonstration (SD&D) effort. During this time, the contractors focused on proving the feasibility of migrating existing DoD technology into the commercial sector and exploring other technology as appropriate. Following Preliminary Design Reviews with all three companies in July 2004, the Phase I portion of the twenty-four month SD&D effort concluded and DHS selected BAE Systems and Northrop Grumman to proceed into Phase II to further mature their preliminary designs, build representative prototypes, install them on aircraft, and conduct formal testing during the Phase II eighteen month effort.

- Involved the commercial aviation stakeholder community beginning in FY 2004 through a widely publicized industry day and a series of one-on-one briefings with key commercial aviation groups and organizations. In late 2004, the Program Office hosted a Stakeholders' Meeting, which was attended by representatives of the airlines, the equipment manufacturers, and other affected sectors, including representatives of multiple Federal government Departments and Agencies.

- Initiated Phase II of the Program. BAE Systems and Northrop Grumman were selected to proceed into this phase. Phase II of the program includes advancing the studies initiated in Phase I, building system prototypes, applying for and receiving FAA certification of system airworthiness, and effectiveness testing.

Office of Safety Act Implementation

- Drafted regulation, commented upon and implemented. Facilities to house the program were selected and the Office has identified and entered into agreements with the lead implementation contractor and lead web site development/management contactor. The Office designed and implemented a web-based application kit and process with an interactive help desk. The Office executed a robust outreach program to introduce the industry to the SAFETY Act program and to encourage its participation. The Office conducted one-day educational seminars across the U.S. inviting industry, attorneys, risk managers and insurance representatives to participate. Articles and interviews were conducted to further our outreach initiatives. To ensure that pending procurement actions are addressed expeditiously and effectively, the S&T Directorate has created a partnership with Federal procurement offices to introduce them to the program; the Office is designing a mechanism that incorporates the SAFETY Act program into the procurement process.
- Received and has taken action on 30 full applications and 120 pre-applications. Four applicants have been awarded SAFETY Act designation and certification: Northrop Grumman, Michael Stapleton Associates, Teledyne Brown Engineering and Lockheed Martin.

Office of Interoperability and Compatibility

- Interviewed key stakeholders across federal and practitioner communities to validate findings, uncover additional interoperability initiatives, and determine key issues for first response; identified a core group of federal programs that test and evaluate first responder equipment; began developing a plan to establish a Joint Evaluation and Testing Program to coordinate with other federal agencies; and conducted an initial scan of existing programs for first responders and collected information at the local, state, and federal levels.

University and Fellowship Programs

- Selected the Texas A&M University and its partners from the University of Texas Medical Branch, University of California at Davis, and the University of Southern California to receive $18 million over the course of the next three years for the study of foreign animal and zoonotic diseases. The Center, which will be known as the National Center for Foreign Animal and Zoonotic Disease Defense, will work closely with partners in academia, industry and government to address potential threats to animal agriculture including Foot and Mouth Disease, Rift Valley fever, Avian influenza and Brucellosis. The Foot and Mouth research will be carried out in close collaboration with DHS's Plum Island Animal Disease Center.

- Selected the University of Minnesota and its partners for the National Center for Food Protection and Defense to address agricultural security issues related to post-harvest food protection. The University of Minnesota's team includes partnerships with major food companies as well as other universities, including Michigan State University, University of Wisconsin at Madison, North Dakota State University and others. The Department of Homeland Security expects to provide the University of Minnesota and its partners with $15 million over the course of the next three years to establish best practices and attract new researchers to manage and respond to food contamination events, both intentional and naturally occurring.

- Selected the University of Maryland and its partners as the site for the fourth Center of Excellence on Behavioral and Social Research of Terrorism and Counter-Terrorism. This Center will be funded at $12 million for three years. Support will continue for the three previously awarded DHS Centers as well. All DHS Centers will have a DHS program manager as well as a technical liaison to facilitate linking research and education objectives with the longer range needs of S&T portfolios and DHS operating Directorates. A reporting and assessment procedure will be developed and implemented to ensure effective communication. Explicit plans will be put in place to integrate and complement the activities of the individual Centers with larger scale objectives.

- Announced the selection of the University of Maryland (UMD) and its partners as the Center for Behavioral and Social Research on Terrorism and Counter-Terrorism. This Center will be funded at $12 million for three years.

- Selected approximately100 students for the 2004 class of DHS Scholars and Fellows bringing the total of students to about 200. Students from the 2003 and 2004 class participated in a DHS orientation for the purpose of learning about DHS mission objectives, the critical research needs, and meeting scientists from DHS laboratories, Centers of Excellence and DOE national laboratories. Students from both classes are attending 93 institutions (including Historically Black Colleges and Universities/Minority Serving Institutions) in 38 states and the District of Columbia. Seventeen of the institutions are located in Experienced Programs to Stimulate Competitive Research (EPSCoR) states. Besides making immediate contributions to homeland security-related R&D, these students will be part of the development of a broad research capability within the Nation's universities to address scientific and technological issues related to homeland security.

- As part of the DHS mission to maximize interaction with other Federal agencies, University Programs and EPA's Science to Achieve Results (STAR) Program have collaborated on the topic of microbial risk assessment. The DHS-EPA Cooperative Center on Microbial Risk Assessment will result in one five year grant to a university-based consortium that is jointly funded by both agencies at $10 million.

Critical Infrastructure Protection

- Developed a CIP Decision Support System (DSS) focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection. The prototype model includes representation of all 14 critical infrastructure sectors, as outlined in the National Strategy for the Protection of Critical Infrastructures and Key Assets, as well as their interdependencies. Preliminary test cases have been used to develop consequence estimation features of the CIP-DSS at both national and metropolitan scales.

- Identified requirements for standards and research and development for Supervisory Control and Data and Acquisition (SCADA) systems.

- Initiated a system study to find potential solutions for personnel surety for security guards that guard our Nation's Critical Infrastructure, as well as insiders with access to sensitive areas of, or information about the infrastructure.

- Began National Research Council studies on the security of the Electrical and Chemical sectors.

- Supported a System Study for Municipal Domestic Water Security, along with the Biological Countermeasures portfolio, Chemical Countermeasures portfolio, and Radiological/Nuclear Countermeasures portfolio.

- Initiated interagency development of the first annual National Critical Infrastructure Protection R&D Plan using the Infrastructure Subcommittee of the National Science and Technology Council.

Cybersecurity

- Initiated dialog aimed at international collaboration on cyber security R&D with Canada, the United Kingdom, and Japan. Interactions with the United Kingdom and Japan are at early stages and have not yet reached the point where potential joint R&D activities have been identified. Interactions with Canada are more advanced, with three joint, mutually synergistic U.S.-Canada R&D projects resulting from the interaction: (1) a secure wireless data pilot project, (2) collaborative funding of an economic assessment study, and (3) development of geographic information system-based tools for geospatial mapping of cyber assets.

- Focused on securing the domain name infrastructure is working to advance the diffusion and use of the Domain Name System Security Extensions (DNSSEC) protocol as a replacement for the traditional domain name infrastructure. Worked with Federal researchers and officials and the private sector to develop a roadmap to accelerate the development and deployment of a secure domain name infrastructure. Current work also includes the identification of technology requirements and development of models to aid in assessing the performance impact of utilizing DNSSEC in operational environments.

- A second effort aimed at secure routing infrastructure is working to address vulnerabilities in Border Gateway Protocol (BGP), the protocol associated with the Internet's underlying routing infrastructure. This need was also identified as a priority in the *National Strategy to Secure Cyberspace*. Focused on preliminary planning for outyear activities. The development and deployment path for a secure routing protocol is expected be similar to that of DNSSEC, but will reach an equivalent level of maturity some years later, with DHS investments aimed at accelerating this process.

- Initiated a research and development program to fund the development of next-generation cyber security technologies in a variety of topic areas including: (1) Vulnerability prevention, discovery and remediation through software assurance technology, including tools for development and code analysis; (2) Cyber security assessment methods and tools, including the development of metrics, security analysis, development of benchmarks; (3) Security and trustworthiness of information systems, with an emphasis on critical infrastructure sectors and critical information infrastructure systems; (4) Wireless security, including foundation for new wireless-based security mechanisms and services, and security for mobile ad hoc wireless networks; (5) Network attack forensics, focused on Internet Protocol traceback (tracing of data back to its source) and attack traceback; and (6) Technologies to defend against identity theft.

- Development of a security architecture for securing the DETER testbed, initial operation of the initial testbed cluster (a scaled-down version of the final testbed), development of an initial hardware/software design document, and initiation of interconnection of university facilities. Accomplishments for the EMIST framework include development of experimental policies and procedures, calibration experiments, operational Phase I experiments on the scaled-down testbed, and documentation of additional attack scenarios and defense mechanisms.

- Initiated a program to address different facets of the need for improved methods for cyber security assessment and testing, in order to provide a foundation for the long term goal of economically-informed risk-based cyber security decision making. Initiated investigations of two important issues. The first is the development of a general model for assessing the economic impact of cyber events and attacks to verify or refute the figures typically publicized (e.g., $38 billion for a single Internet worm attack). The second area of interest is the development of tailored business cases aimed at different types of stakeholder community perspectives (e.g., large enterprises, critical infrastructure sector companies, small businesses, home users, etc.). These activities are aimed at putting better information in the hands of cyber security decision makers (ranging from policy makers to customers of commercial security technology).

- Development of a trusted access information sharing repository infrastructure for collecting and sharing data sets among trusted partners, and development of a contractual and policy framework for ensuring trust among participants and protection of data sets through the Large-scale Network Data Sets Program.

Appendix B

S&T Directorate Interagency Interactions

Department of Homeland Security

March 2004 to February 2005

International:

The Science & Technology Directorate led the interagency effort to pilot a distributed database architecture to support verification of the identity of international travelers and validity of their travel documents. Primary partners on this effort are DHS, OSTP, DOS, and DOJ.

The S&T Directorate worked with DOS (STAS), USDA, OSTP, NSF to create and support the US-Japan Safe and Secure Society forum.

The Directorate and DOS (OES) jointly created and negotiated the US-UK S&T Memorandum of Agreement (MOA). The resulting MOA supports collaboration on Homeland Security research, development, testing, and evaluation between the US and the UK.

The S&T Directorate has partnered with DOE (Second Line of Defense) and the UK to conduct information exchanges regarding development and operational testing of radiation monitors for border security applications.

Biological Countermeasures:

The Science and Technology Directorate participated in the White House led interagency Homeland Security Council (HSC) Biodefense Pathobiologics Collaborating Center. This committee has played a major role in conducting the Biodefense End-to-End Study which then led to HSPD-10, NSPD-33 and is now overseeing the implementation of that HSPD/NSPD. Separate subcommittees of this PCC have addressed Food, Agricultural, and Water Security.

The Science and Technology Directorate enacted Project BioShield was enacted in 2004 as a joint HHS-DHS program to accelerate the development of new medical countermeasures for biological, chemical and radiological/nuclear threats.

The Science and Technology Directorate is a co-chair on the Weapons of Mass Destruction Medical Countermeasures (WMD-MCM) subcommittee. This is a subcommittee under the National Science and Technology Council, and has been providing input on BioShield needs and recommendations. DoD and HHS are the primary partners on this subcommittee.

The Science and Technology Directorate and HHS co-chair an interagency committee to address the Engineered Threat.

The Science and Technology Directorate is developing the National Biosurveillance Integration System (NBIS) to integrate biosurveillance information from interagency partners into a common operating picture and then share that information with Federal, state and local partners.

The Science and Technology Directorate leads a partnership with CDC, EPA, and FBI on the deployment of BioWatch, a bioaerosol detection system deployed to many of this nation's cities.

BioNet is a DHS funded, DTRA executed pilot program to integrate civilian and military domestic biodetection and consequence management, using San Diego as a pilot city.

As part of its HSPD-10 responsibility, the Science and Technology Directorate is leading an interagency effort with HHS, DoD, and USPS to develop a National Integrated Biomonitoring System.

The Science and Technology Directorate is a primary participant in the establishment of the National Interagency Biodefense Campus being developed at Ft. Detrick.

The National Bioforensics Analysis Center (NBFAC) is a joint Science and Technology Directorate-FBI program.

The Science and Technology Directorate and USDA have developed an integrated national agrodefense strategy, with especial emphasis on foreign animal disease. The Directorate and USDA also conduct joint research and development programs at the Plum Island Animal Disease Center.

Chemical Countermeasures:

The Science and Technology Directorate participated an interagency effort lead by the Homeland Security Council (HSC) to define the nation's operational vulnerabilities and gaps in responding to a chemical terrorist attack. Interagency participants on this effort include DOD, HSC, OMB, HHS, OSTP, NSC, DHS, EPA, VA, USDA, OVP, FBI, DOT, DOL, and TSWG. The interagency working group has completed a draft version of a Chemical End-to-End Assessment that identifies critical gaps and vulnerabilities in the nation's chemical defense.

The Science and Technology Directorate participated on the Counterproliferation Technology Coordinating Committee Chemical Weapons Working Group with other interagency partners, including DOD, EPA, TSWG, HHS, CIA, and DIA. The CTCC was created to improve the coordination of WMD R&D efforts among government agencies. The CTCC Chemical Weapons Working Group meetings resulted in the development of a document identifying priorities, gaps and overlaps in existing R&D programs.

The Science and Technology Directorate initiated an interagency technical working group focused on the establishment of an Environmental Chemical Laboratory Response Network. Interagency partners in this effort include DoD, EPA, CDC, FBI, CIA, HSC, OSTP, and OVP.

The Science and Technology Directorate is a leading member of a technical working group to establish CSAC. The CSAC will provide the nation with the scientific basis for awareness of chemical threats and attribution of their use against the American public and involves knowledge management, threat characterization, and forensics. The interagency partners in this effort include DoD, CIA, DIA, and the FBI. Currently, efforts are focused on the development of MOUs between DHS and DoD and DHS and the Intelligence Community.

The Science and Technology Directorate is a member of the Scientific Working Group for Forensic Analysis of Chemical Threats (SWGFACT). Interagency partners participating in SWGFACT include DoD, DOE, FBI, CDC, FDA, and USDA.

The Science and Technology Directorate participated jointly lead an effort with OSTP to develop an interagency report to shape strategy and provide guidance regarding WMD research and development. Agencies involved in this effort include DoD, EPA, TSWG, CDC, FDA, and NIH. This effort resulted in a National Strategy for Chemical Defense that outlined necessary efforts by participating agencies.

Explosives Countermeasures:

The Science and Technology Directorate organized an IED Working Group that has included representatives from DOS, DOT, DOI, DoD, DOJ, DOE, Joint IED Task Force. This meeting allows each agency a forum to discuss their requirements and plans with regard to IEDs. Discussions focus on Science and Technology Department mandates, the IED organization roles and responsibilities, partnerships, resources, operational and technical requirements, plans for FY05 and out years, specific projects, technologies of interest, and outcomes/lessons learned.

The Science and Technology Directorate sponsored a VBIED conference, attended by representatives of the DOS, DOT, DOD (including OSD, OCJCS, USN, USA, USAF, PSEAG, DTRA), DOE, DOJ, FBI, and NIJ. This conference provided a forum to share information on detection approaches with the community and encourage provocative discussions among peers.

The Science and Technology Directorate is sponsoring a suicide bomber conference scheduled for February 2005. The primary focus of this meeting will center on the detection of suicide bombers. Speakers from appropriate government agencies will present information about the technologies, both existing and those in developmental stages, qualified for detecting explosives carried on the person.

The Science and Technology Directorate has worked closely with TSWG and DoD in their efforts to address the explosives threat, including participation in conferences, technical evaluations, program reviews, and site visits.

Radiological/Nuclear Countermeasures:

The Science and Technology Directorate hosted an interagency Technical Exchange Meeting to provide a forum for interagency communication on Radiological and Nuclear Countermeasures research and development.

The Science and Technology Directorate participated in several exchanges with DOE components working the radiological/nuclear area to consolidate efforts.

The Science and Technology Directorate participated on the OSTP Domestic Nuclear Defense Working Group to facilitate the formation of the Domestic Nuclear Defense Office.

The Science and Technology Directorate has a lead role in the establishment of the DNDO. The DNDO is being stood up as a national office that will be comprised of interagency participants. The office will be located within the Department of Homeland Security (DHS), but will be jointly staffed with representatives from DHS, the Department of Energy (DOE), the Department of Defense (DOD), and the Federal Bureau of Investigations (FBI), with coordination between the Department of Justice (DOJ), the Department of State (DOS), the Intelligence Community (IC), and other departments as needed. Interagency staff will hold principle management positions within the DNDO when it becomes fully operational.

Standards:

The Science and Technology Directorate interfaces with other government agencies to facilitate the development of standards for Homeland Security concerns. The Directorate's interactions with other agencies resulted in several voluntary consensus standards developed in concert with US industry and accredited Standards Development Organizations (SDOs).

The Science and Technology Directorate collaborated with DOD (Army, Navy), DOE (National Labs), USDA, and DOC/ National Institute of Standards and Technology) and developed standards for radiation detectors for radiological & nuclear countermeasures.

The Science and Technology Directorate collaborated with DOC/NIST, HHS/Centers for Disease Control, DOD (Office of the Secretary, Army and Navy), FDA, USDA, EPA and FBI to address detection standards for *Bacillus anthracis* (anthrax). This interagency interface resulted in the development of standards for detection of *Bacillus anthracis* (anthrax).

The Science and Technology Directorate succeeded in developing standards for personal protective equipment for emergency responders through collaborative interagency efforts with DOD (Edgewood and Natick), the DOC/NIST, and HHS/NIOSH (Pittsburgh laboratory).

The Science and Technology Directorate developed standards for biometrics (facial photograph standards) by partnering with DOC/NIST, DOJ/FBI and Department of State.

The Science and Technology Directorate participates on an OSTP/NSTC Subcommittee on Standards that included DHS, National Research Council, Environmental Protection Agency, Department of Energy, Health and Human Services/National Cancer Institute, DOL/Occupational Safety and Health Administration and Department of Defense. This Subcommittee on Standards developed Protective Action Guides to provide federal guidance to emergency responders to a dirty bomb or nuclear.

Border and Transportation Security:

The Science and Technology Directorate regularly interfaces with the Department of Justice personnel and is involved in various National Institute of Justice (NIJ) Office of Science and Technology activities. NIJ convenes a technology review board which enables technology transition. NIJ also has a Southwest Center of Excellence for Public Safety Technology. The Directorate has been involved in the University of Houston's educational workshop which is part of the NIJ Center of Excellence.

The Directorate is also in the process of setting up a formal interface with the Federal Bureau of Investigation. The FBI's R&D director is a newly created position, and the Directorate anticipates meeting to discuss areas of collaboration, technology information exchange, and technology transition.

Over the past two years, the Science and Technology Directorate has coordinated extensively with the Department of Defense and Federal Aviation Administration with respect to Unmanned Aerial Vehicle (UAV) operations and evaluations. Last year, the UAV Executive Steering Group (UAV ESG) was established to advise the Secretary of Homeland Security and provide a forum for communication, coordination and cooperation to address DHS UAV issues. The UAV ESG is made up of representatives from DHS components, the Department of Defense and the Federal Aviation Administration.

The Science and Technology Directorate is a representative on the InfoSec Research Council (IRC). The IRC is an interagency working group that engages in coordination activities at a more technical level than the CIP IWG. The IRC is updating the *InfoSec Hard Problems List*, a report on important information security research challenges that was first published in 1999 and is in need of updating due to the significant advances and evolution in technology in the past five years.

The Science and Technology Directorate and NSF are jointly co-funding the two large multi-university projects that form a Cyber Security Testbed Program and recently co-sponsored a United States-Japan Experts Workshop on Critical Information Infrastructure Protection.

Emergency Preparedness and Response:

The Science and Technology Directorate established the Interagency Modeling and Atmospheric Assessment Center (IMAAC) in April 2004. The IMAAC is currently operational and provides atmospheric hazards predictions for incidents of national significance. Participants include DoD, DOE, EPA, NRC, NOAA, NASA, and DOC. The IMAAC developed an MOU that establishes general operating principles and provides for the development of annexes which detail the department to agency specific resource commitments. In addition to the MOU the working group has produced an interim Standard Operating Procedure, currently is reviewing the template for annexes, and started discussions on other critical aspects of atmospheric hazard prediction that will improve the coordination of federal assets.

The Science and Technology Directorate participates in the Federal Committee for Meteorological Services and Supporting Research (FCMSSR). This interagency group provides direct policy guidance to the Office of Federal Coordinator for Meteorological Research

The Science and Technology Directorate participates on the Interdepartmental Committee for Meteorological Services and Supporting Research (ICMSSR) and co-chairs an interagency Joint Action Group as part of this committee. A collaborative process was co-led by the Directorate and the Army Research Office, with participation from DOE, DTRA, Dugway Proving Grounds, EPA NASA, NOAA, and the NRC to focus on modeling of Atmospheric Transport and Dispersion (ATD). The Joint Action Group, as a subset of the ICMSSR, developed an Atmospheric Transport and Diffusion Research and Development Plan that describes the requirements to meet ATD user-community needs. The R&D Plan also recommends strategies to address those needs to achieve reliable ATD modeling capability.

Critical Infrastructure Protection:

The S&T Directorate co-chairs the Infrastructure Subcommittee (ISC) of the National Science and Technology Council (NSTC), and over twenty other government agencies are members of the ISC. The ISC reports directly to two NSTC committees: the Homeland and National Security (co-chaired by the Directorate) and the Technology committees. The ISC developed the first annual 2004 National CIP R&D Plan as well as hosted a Federal CIP R&D Managers Workshop focused on drafting the 2005 National CIP R&D Plan.

The Directorate is co-sponsoring a multi-agency (including non-government) CIP Roundtable with the National Academy of Sciences that will begin meeting in the upcoming year. The roundtable is aimed at addressing the most pressing vulnerabilities associated with critical interdependent infrastructure systems. A dialogue between government, industry, and academia will be established to facilitate development of a long-term strategy for reducing the vulnerability of the nation's infrastructure to debilitating failures, whether from terrorist acts, natural disasters, or accidental failures.

The Science and Technology Directorate is a member of the DoD Defense Science Board Task Force on Critical Homeland Infrastructure Protection. The Defense Science Board (DSB) on Critical Homeland Infrastructure Protection (CHIP) has concluded their assessment of US Homeland Installations, and is in the process of writing a report on identifying issues for balancing military and private responsibilities for Critical Facility Protection. The report will also address shortfalls and deficiencies associated with operational security, and gaps in security standards.

The Science and Technology Directorate is an ex-officio member of the Government Coordinating Council for Nuclear Power Plants. This Council is one of the entities established by the National Infrastructure Protection Plan (NIPP). In a joint effort, the Nuclear Power Plant and Disposal Facilities Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) is conducting Comprehensive Reviews on all of the Nation's Nuclear Power Plants used for commercial power generation. These reviews include Buffer Zone Protection Plans, Site Security Plans, Nuclear Site Security Annexes, On-Site Emergency Preparedness

Plans, Off-site Emergency Preparedness Plans, and consideration of the general vulnerability to an aircraft as a weapon.

Cyber Security:

The Science and Technology Directorate co-chairs the Critical Information Infrastructure Protection Interagency Working Group (CIIP IWG). The CIIP IWG is chartered by the White House Office of Science and Technology Policy (OSTP) under the National Science and Technology Council (NSTC) and is co-chaired by OSTP. The CIIP IWG has membership from more than twenty organizations in over a dozen departments and agencies, meets monthly, and is developing a coordinated interagency Federal Cyber Security R&D Plan to guide future funding and programmatic decision making in this area.